(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2000－503198
（P2000－503198A）
(43)公表日　平成12年３月14日(2000.3.14)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｚ	
12/28		Ｈ０４Ｍ　3/00	Ｂ	
12/46		11/00	３０３	
12/66		Ｈ０４Ｌ　11/20	Ｂ	
29/08		13/00	３０７Ｚ	

審査請求　有　　予備審査請求　未請求(全 53 頁)　最終頁に続く

(21)出願番号　特願平11－507419
(86)(22)出願日　平成10年７月２日(1998.7.2)
(85)翻訳文提出日　平成11年３月３日(1999.3.3)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／１３８５８
(87)国際公開番号　ＷＯ９９／０１９６９
(87)国際公開日　平成11年１月14日(1999.1.14)
(31)優先権主張番号　０８／８８７，３１３
(32)優先日　平成９年７月３日(1997.7.3)
(33)優先権主張国　米国（ＵＳ）

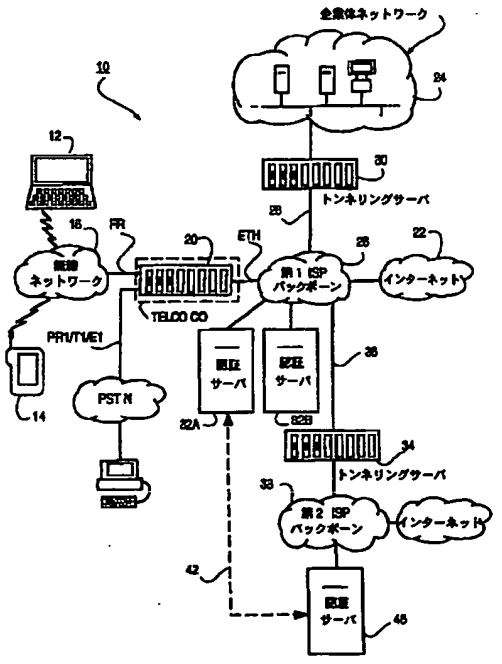
(71)出願人　スリーコム　コーポレイション
アメリカ合衆国　イリノイ　ローリング　メドウズ　ゴルフ　ロード　3800
(72)発明者　ユイ　イーチュン
アメリカ合衆国　イリノイ　パファロー　グローヴ　チェスナット　コート　ウェスト　36
(72)発明者　ベネット　エス　カードウェル
アメリカ合衆国　イリノイ　エヴァンストン　リース　アヴェニュー　2749
(74)代理人　弁理士　矢野　敏雄　（外２名）

最終頁に続く

(54)【発明の名称】　インターネットへのダイレクトワイヤレスアクセスを含む、ネットワークアクセス方法

(57)【要約】
ディジタルデータ源をコンピュータネットワークに接続する方法。ディジタルデータ源はワイヤレス伝送オフアクシス伝送媒体を介してワイヤレスサービスキャリアにデータを伝送し、ワイヤレスサービスキャリアにより該データが多重化され高速ディジタル電話回線に送出される。この方法は以下のステップ：ディジタルデータをネットワークアクセスサーバ等の通信シャシにおいて受け取り、該ディジタルデータから、少なくとも（ａ）ディジタルデータ源の呼び出した電話番号又は（ｂ）ディジタルデータ源に関連した電話番号を含むネットワークアクセス認証データを抽出し；認証データを、該コンピュータネットワーク用のネットワーク認証サーバに接続されたローカル又はワイドエリアコンピュータネットワークを介して伝送し；ネットワーク認証サーバにおいて、伝送された認証データに基づいて該遠隔ユーザに対してコンピュータネットワークへのアクセスが許可されているかどうかを判断し；認証サーバは認証アクセスサーバに対して判断ステップの結果を通知し：判断ステップの結果が肯定であればデータ源に対してコンピュータネッ

FIG. 1



【特許請求の範囲】

１．デジタルデータ源をコンピュータネットワークに接続する方法において、前記ディジタルデータ源はワイヤレス伝送媒体を介してワイヤレスサービスキャリアと通信を行い、前記ワイヤレスサービスキャリアは前記ディジタルデータを多重化し高速ディジタル電話回線に送出するよう構成されており、前記方法が

前記ディジタルデータを、電話回線インタフェース及びネットワークインタフェースを有する通信装置において受け取り、

前記通信装置は前記ディジタルデータからアクセス認証データを抽出し、前記認証データは少なくとも（ａ）前記ディジタルデータ源により呼び出された電話番号、又は（ｂ）前記ディジタルデータ源に関連付けられた電話番号のいずれかを有し、

前記通信装置は前記認証データを、前記ネットワークアクセスサーバに接続されたローカルエリア又はワイドエリアコンピュータネットワークを介して、前記コンピュータネットワーク用のネットワーク認証サーバに伝送し、

前記ネットワーク認証サーバ内において、前記伝送された認証データに基づいて、前記遠隔ユーザが前記コンピュータネットワークに対してアクセス許可されているかどうかを判断し、

前記認証サーバは、前記通信装置に対して、前記判断ステップの結果を通知し、判断結果が肯定的であれば前記コンピュータネットワークに対するアクセスを前記ディジタルデータ源に許可する、という各ステップを有していることを特徴とする方法。

２．前記認証サーバにおいて、前記通信装置に結合されており、前記ディジタルデータ源に対して前記コンピュータネットワークへのアクセスを与えるためのトンネリングサーバを識別し、

前記ディジタルデータ源からのディジタルデータを前記トンネリングサーバにルーティングすることにより、前記アクセスを前記コンピュータネットワークに与えるステップを更に有した、請求項１記載の方法。

３．前記認証サーバにおいて、前記ディジタルデータ源のための、すなわち前

記ディジタルデータを前記ネットワークアクセスサーバと前記トンネリングサーバとの間でトンネリングするためのトンネリングプロトコルを決定し、

前記ディジタルデータ源からのディジタルデータを前記トンネリングプロトコルに従って前記トンネリングサーバにルーティングするステップを更に有した、請求項２記載の方法。

４．前記トンネリングプロトコルが、ＰＰＴＰ及びＴＥＬＮＥＴを含むプロトコル群から選択される、請求項２記載の方法。

５．前記コンピュータネットワークがインターネットを含む、請求項１記載の方法。

６．前記コンピュータネットワークが企業ローカルエリア又はワイドエリアネットワークを含む、請求項１記載の方法。

７．前記通信装置が公衆交換電話網にアクセスを供給し、前記通信装置は、前記判断ステップにおいて否定的反応が得られた場合に、前記公衆交換電話網を介して前記ディジタルデータを目的地にルーティングするよう試みるよう構成された、請求項１記載の方法。

８．（１）前記トンネリングサーバ又は（２）前記認証サーバと前記ディジタルデータ源との間でパスワード認証ルーチンを実行し、前記ディジタルデータ源と前記コンピュータネットワーク間で第２レベルの認証を行うよう構成された、請求項２記載の方法。

９．高速電話回線を介してユーザからの電話呼出を受け取るよう構成された通信装置を有したインターネットサービスプロバイダのためのインターネットアクセス方法において、

前記通信装置を、ローカル又はワイドエリアネットワークを介して認証サーバに接続し、

前記ユーザからの入力呼出から、少なくとも（ａ）前記ユーザにより呼び出された電話番号又は（ｂ）前記ユーザに関連付けられた電話番号のいづれかを有するネットワークアクセス認証データを抽出し、

前記ネットワーク認証データを前記認証サーバにルーティングし、前記ネットワークアクセス認証データに基づいて前記ユーザの認証を行い、

前記ユーザに対してネットワークアクセスを与えるためのトンネリングサーバを識別し、前記ネットワークアクセスサーバに前記トンネリングサーバを通知し、

前記ネットワークアクセスサーバからのディジタルデータを前記トンネリングサーバにトンネリングし、

前記トンネリングサーバにより前記ディジタルデータをインターネットに送る、という各ステップを有した方法。

１０．前記トンネリングステップにおいて前記ユーザのためのトンネリングプロトコルを識別するステップを更に有した、請求項９記載の方法。

１１．ディジタルデータを発生するコンピュータをインターネットに接続する方法において、前記ディジタルデータは高速ディジタル電話回線を介してインターネットサービスプロバイダに伝送されるよう構成されており、

前記ディジタルデータを、前記インターネットサービスプロバイダの通信装置において受け取り、

前記ディジタルデータから、少なくとも（ａ）前記ディジタルデータ源により呼び出された電話番号又は（ｂ）前記コンピュータに関連付けられた電話番号のいづれか、を有するインターネットアクセス認証データを抽出し、

前記認証データをネットワーク認証サーバに伝送し、

前記ネットワーク認証サーバ内で、前記伝送された認証データに基づいて、前記遠隔ユーザが前記ネットワークアクセスサーバを介してインターネットにアクセスすることが許可されているかどうかを判断し、

前記認証サーバは前記ネットワークアクセスサーバに、前記判断ステップの結果を通知し、前記判断ステップにおいて肯定的反応が得られた場合は前記コンピュータに対してインターネットへのアクセスを許可する、という各ステップを有した方法。

１２．コンピュータがインターネットにアクセスするために使用するトンネリングサーバを、前記認証サーバ内で識別し、

前記コンピュータからのディジタルデータを前記トンネリングサーバにルーティングし、インターネットへの前記アクセスを供給するという各ステップをさらに有した、請求項１１記載の方法。

１３．前記認証サーバにおいて、前記ネットワークアクセスサーバと前記トンネリングサーバ間でディジタルデータをトンネリングするために使用するトンネリングプロトコルを決定し、

前記コンピュータからのディジタルデータを、前記トンネリングプロトコルに従って前記トンネリングサーバにルーティングするという各ステップを更に有した、請求項１２記載の方法。

１４．前記トンネリングプロトコルが、ＰＰＴＰ及びＴＥＬＮＥＴを含むプロトコル群から選択される、請求項１３記載の方法。

１５．前記通信装置が公衆交換電話網にアクセスを供給し、前記通信装置は、前記判断ステップにおいて否定的反応が得られた場合には前記公衆交換電話網を介して前記ディジタルデータを目的地にルーティングするよう試みるよう構成されている、請求項１１記載の方法。

１６．（１）前記トンネリングサーバ又は（２）前記認証サーバと前記コンピュータとの間でパスワード認証ルーチンを実行し、前記ディジタルデータ源と前記コンピュータネットワークとの間で第２レベルの認証を実行するよう構成された、請求項１２記載の方法。

１７．ワイヤレスインターネットユーザのためのインターネットサービスプロバイダシステムにおいて、

ネットワークアクセスサーバと、

インターネットアクセス認証サーバとを有し、

前記ネットワークアクセスサーバは高速ディジタル電話回線インタフェースとインターネットゲートウェイを有し、該インタフェースは前記ワイヤレスインターネットユーザからの呼出を受け取り、該ゲートウェイは、前記ワイヤレスイン

ターネットユーザに関連付けられたディジタルデータをインターネットに送出し、

前記インターネットアクセス認証サーバは通信媒体を介して前記ネットワークアクセスサーバに接続され、前記インターネットアクセス認証データに応答するよう構成され、該認証データは、前記ワイヤレスインターネットユーザに関連付けられた前記ディジタルデータから抽出され、また前記ディジタルデータは前記ネットワークアクセスサーバにより受け取られ前記認証サーバに伝送されたものであり、

前記認証サーバはさらにメモリを備え、それによって、前記インターネットアクセス認証データに基づいて、前記ワイヤレスインターネットユーザがインターネットに対してアクセス許可されているかどうかを判断し、前記インターネットサーバは前記ネットワークアクセスサーバに認証反応を送信し、

前記ネットワークアクセスサーバは前記認証サーバからの前記認証反応に応答し、前記ワイヤレスインターネットユーザに対してインターネットへのアクセスを許可するが、又は該ワイヤレスインターネットユーザからの呼出に関してその他の動作を行うよう構成された、インターネットサービスプロバイダシステム。

１８．前記ネットワークアクセスサーバと通信媒体を介して結合された第２インターネット認証サーバを有し、

前記第２インターネット認証サーバは前記ネットワークアクセスサーバからの認証データに反応するよう

構成され、また第２のインターネットサービスプロバイダにより管理され、

更に前記第２インターネット認証サーバは前記ワイヤレスインターネットユーザに対して、前記ネットワークアクセスサーバ又は前記インターネットアクセス認証サーバの何れかに対する認証反応を与えるよう構成されている、請求項１７記載のインターネットサービスプロバイダシステム。

【発明の詳細な説明】

インターネットへのダイレクトワイヤレスアクセスを
含む、ネットワークアクセス方法

発明の背景

Ａ．発明の分野

この発明はデータ通信の分野に関し、特にワイヤレスユーザにより発生されたディジタルデータ（携帯電話モデムを有したコンピュータ等）を、社内ＬＡＮやインターネットなどのコンピュータネットワークに接続する方法に関する。

Ｂ．関連技術の説明

公衆交換電話網からダイヤルしている遠隔ユーザに対してローカル又は広域ネットワークへのアクセスを可能にするネットワークアクセスサーバが公知である。このような装置は３ＣＯＭ社（以前はU.S.Robotics Access Corp.）、すなわち本願の譲受人から入手可能である。３ＣＯＭ社の総合制御ネットワーク企業体ハブ（Total Control Network Enterprise Hub）が代表的なネットワークアクセスサーバである。このサーバは、Baum他の米国特許第５５７７１０５号：「データ通信用の電話呼出交換及びルーティング方法」に、また、Walsh他の米国特許第５５２８５９５号：「モデム

入出力信号処理方法」に記載されている。Walsh他及びBaum他の特許は何れも本願明細書に引用する。

Walsh等及びBaum等の特許に記載されたネットワークアクセスサーバは、多重ディジタル電話回線へのインタフェース、遠隔ユーザからのデータを信号変換するための複数のモデム、及びモデムからの復調データをローカル又はワイドネットワークへ伝送するためのネットワークインタフェースを有する。時分割多重バスを有する高速ミッドプレーンバス構造は、電話回線のチャネルとモデム間の信号路として機能する。この高速ミッドプレーンは、モデムとネットワークインタフェースを結合する並列バスも含む。

単一のシャシにおけるこのネットワーク・アクセス・サーバ・アーキテクチャは様々なアプリケーション、特に企業ネットワークアクセスの分野において非常

に人気が高い。このネットワーク・アクセス・サーバ・アーキテクチャはまた、陸上インターネットユーザに対するインターネットサービスプロバイダにも人気が高い。１つのネットワークアクセスサーバにより、インターネットサービスプロバイダは多数の同時インターネットアクセス呼出に対処し、複数の遠隔ユーザとインターネット上のホストコンピュータ間において全二重通信を供給することができる。

ワイヤレスユーザに対してインターネットアクセスを可能にする技術が出現しつつある。ワイヤレスサー

ビスには２つの競合する標準、すなわちＣＤＭＡ（符号分割多重アクセス。標準文書ＩＳ－１３０及びＩＳ－１３５に記載。参照として本願明細書に引用。）と、ＴＤＭＡ（時分割多重アクセス。標準文書ＩＳ－９９に記載。同じく参照として本願明細書に引用。）がある。これらの標準は、音声とデータ両方のための機能の豊富なディジタル無線通信の形式を規定している。この２つの標準は、複数のユーザからのディジタルデータがどのように無線インターフェース上で多重化されるかという点で異なる。

いずれの無線技術においても、ワイヤレスユーザはデータを移動交換センタへ送信する。移動交換センタは公衆交換電話網に対する接続を可能にし、特定の多重・制御機能を果たし、移動ユーザに対して交換機能を提供する。それによって、複数のワイヤレスユーザからの多重化ディジタルデータを高速通信フォーマット（フレームリレー等）を介して、公衆交換電話網内の通信要素に送ることが可能となる。

本願の発明は、特にワイヤレスユーザに適した、ネットワークアクセス方法及び装置を提供する。本願発明のネットワーク・アクセス方法によれば、ネットワークアクセスサーバと、１つ又は複数の認証サーバが協働して、インターネット及び企業ネットワーク認証及びアクセスを供給することが可能となる。ネットワークアクセスサーバは、ＴＤＭＡ又はＣＤＭＡ移動電

話に接続された端末装置と、公衆交換電話網（ＰＳＴＮ）及びインターネットに

接続された端末装置とが協働するために必要な機能を供給する。さらに、本発明によれば、複数のインターネットサービスプロバイダに加入している複数の遠隔ユーザのためのインターネットアクセス方法が提供され、インターネットサービスプロバイダは様々なインターネットユーザに対してより柔軟なサービスを提供することが可能となる。

発明の要旨

ディジタルデータの発生源をコンピュータネットワークに接続する方法が提供される。このディジタルデータ源ははディジタルデータを発生するとともに、ワイヤレス送信媒体を介してワイヤレスサービスキャリアとの通信を行う。ワイヤレスサービスキャリアはディジタルデータを高速ディジタル電話回線上に多重化し、ネットワークアクセスを供給する通信シャシ又はサーバに送信する。本発明の方法は通信シャシ上でディジタルデータを受け取り、ディジタルデータから、少なくとも、（ａ）ディジタルデータ源により呼び出された電話番号、又は（ｂ）ディジタルデータ源と関連付けられた電話番号、のうち１つを含むネットワークアクセス認証データを取り出す。通信シャシは、ネットワークアクセスサーバに接続されたローカルエリア又はワイドエリアコンピュータネットワークを介して、認証データを、コンピュータネットワーク用のネットワーク・認証・サーバに送信する。ネットワーク認証サーバは送信された認証・データに基づいて、遠隔ユーザがコンピュータネットワークにアクセスすることが許可されているかどうかを判断する。認証サーバは従って、ネットワークアクセスサーバに判断の結果を知らせる。遠隔ユーザは、判断ステップの結果が肯定であれば、コンピュータネットワークへのアクセスが許可される。

この方法はさらに、ローカルエリア又はワイドエリアネットワークを介して通信シャシにリンクされたトンネリングサーバを認識し、データ源からのディジタルデータをトンネリングサーバにルーティングしてコンピュータネットワークへのアクセスを供給するステップを含むことができる。前記トンネリングサーバはディジタルデータ源に対して、コンピュータネットワークへのアクセスを与えるものである。トンネリングサービスの識別は遠隔ユーザからの認証データに基づ

いて行われ、該データは遠隔ユーザの電話番号やダイアルされた番号等である。この実施例では、認証サーバにおいて、ディジタルデータ源からのディジタルデータを通信装置とトンネリングサーバ間でトンネリングするためのトンネリングプロトコルを決定することもできる。この決定ステップは、例えば、遠隔ユーザ（該ユーザの電話番号等により識別）に関連付けられ

たトンネリングサーバと必要なプロトコルをソフトウェアルックアップテーブルから見つけだすことにより実行可能である。ディジタルデータはトンネリングプロトコルに従って、トンネリングサーバを介してルーティングされる。好適な実施例では、ＰＰＴＰ又はＴＥＬＮＥＴプロトコルが使用される。

アクセス認証の第２段階がオプションとして行われる。これは、遠隔ユーザと認証サーバ又はトンネリングサーバ間で行われるパスワード認証ルーチンから構成される。

本発明の主要な目的は、従って、ワイヤレスユーザ等の遠隔ユーザに対して、インターネットその他のコンピュータネットワークへの直接的アクセスを供給することである。この目的及びその他の目的は以下の詳細な説明から明らかとなる。

図面の簡単な説明

現在のところ好適と考えられる本発明の実施例を図面を参照して説明する。図面において、同一の参照番号は同一の要素を示す。

図１は本発明の実施例におけるワイヤレスユーザ用に好適なネットワークアクセスシステムの一例である。

図２は、図１の通信シャシの好適な一形態の機能ブロック図である。該通信シャシはワイヤレスユーザのみならず、公衆交換電話網を介してダイアルするユーザをも取り扱うことができる。

図２Ａは、アナログモデム呼出に対応していない実施例に適した通信シャシのブロック図である。

図３は、遠隔ユーザと図１のトンネリングサーバ間のトンネルインタフェース

用プロトコルスタックである。

図４は、通信シャシと図１の認証サーバ間の認証及び課金インタフェース用のプロトコルスタックである。

図５は、リモートダイアルユーザと、該ユーザを目的地端末装置に接続するルータとの間の非トンネリングインタフェースのプロトコルスタックである。

図６は本発明の好適な実施例における、呼出受入シナリオにおけるトンネリング用ＰＰＴＰプロトコルの呼出フローである。

図７は本発明の好適な実施例における、呼出受入シナリオのトンネリング用ＴＥＬＮＥＴプロトコルの呼出フローである。

図８は、認証失敗シナリオにおける呼出フローである。

図９は、トンネリングサーバアクセス拒絶シナリオにおける呼出フローである。

図１０は、ＰＰＴＰプロトコルにおいてログインパスワード認証がネットワークアクセス認証プロシージャの第２段階として実行された場合における、認証失敗シナリオの呼出フローである。

図１１は、ＴＥＬＮＥＴにおいてログインパスワード認証がネットワークアクセス認証プロシージャの第２段階として実行された場合における、認証失敗シナリオの呼出フローである。

好適な実施例の詳細な説明

図１には、本発明の実施に好適なネットワークアクセスシステム１０が示されている。このシステムは無線装置１２、１４のユーザにより使用される。無線モデムを備えたラップトップコンピュータ、又は無線パーソナルデータアシスタント（ＰＤＡ）１４等の遠隔装置は、無線モデムを介して、ＴＤＭＡ（時分割多重アクセス）又はＣＤＭＡ（符号分割多重アクセス）標準に従って、無線ディジタル通信ネットワークと通信を行う。

ワイヤレスネットワーク１６はモバイルスイッチングセンタ（ＭＳＣ）（図示しない）を含む。移動交換センタは無線通信ネットワーク１６内の要素であり、

ワイヤレスユーザに対して公衆交換電話ネットワークへの接続、制御機能及び交換機能を提供する。図１の実施例では、ワイヤレスユーザからのデータはＭＳＣにより高速ディジタルフレームリレー回線ＦＲに乗せられ、ローカル呼び出しエリア内の通信シャシ２０に送信される。好適な実施例では、通信シャシ２０は３Ｃｏｍ社（前身はU. S. Robotics）の総合制御ネットワーク企業体ハブ（Total Control Network Enterprise Hub）等の統合ネットワークアクセスサーバを有する。この場合、該サーバはフレームリレー回線ＦＲとインターフェースし、後述するトンネリング、認証、及びアカウンティング機能を行うよう修正される。

通信シャシ２０は、ＣＤＭＡ／ＴＤＭＡワイヤレスネットワーク１６とインターネットサービスプロバイダ（ＩＳＰ）バックボーンネットワーク２６、インターネット２２又はその他のローカルエリアネットワークＥＴＨとインターネットサービスプロバイダバックボーンネットワーク２６間のゲートウェイとして機能する。シャシ２０は、ＣＤＭＡ又はＴＤＭＡ移動電話に接続された端末装置がＰＳＴＮ及びインターネットネットワークに接続された端末装置と相互に通信を行うために必要な機能を提供する。好適な実施例では、通信シャシ２０は電話会社本社（telephone companay central office; TELCO CO）内に配置され、インターネットサービスプロバイダ（ＩＳＰ）により維持される。シャシ２０はワイヤレスユーザ１２、１４からの呼び出しをワイヤレスネットワーク１６内のＭＳＣを介して、回線ＦＲ上のローカル呼び出しとして受け取る。

無線端末１２、１４は企業／個人ネットワーク２４にアクセスするために、通信シャシ２０とトンネリングサーバ３０間のＬＡＮ又はＷＡＮ回線２８を介して、トンネリングプロトコルを利用する。トンネリングサーバは企業／プライベートネットワーク２４に接続され、かつバックボーンネットワーク２６を介して通信シャシ２０に接続されている。好適な実施例では、トンネリングは、一般に入手可能であるＲＦＣ文書で

あるＰＰＴＰＲＦＣ（１９９６年６月）に記載されたポイントツーポイント・トンネリングプロトコル（ＰＰＴＰ）に従う。このＲＦＣ文書は参照として本願明

細書に引用する。トンネリングは勿論、その他の登場しつつある同等のプロトコル、例えばＬ２ＴＰに従うことも可能である。ＰＰＴＰとＬ２ＴＰは非ＰＰＰ非同期プロトコルを支援するよう設計されていないので、非ＰＰＰ非同期トラフィックを回線２８上でトンネリングするためにはＴＥＬＮＥＴプロトコルを使用する。トンネリングサーバはまた、好適には、前述のトータル・コントロール・エンタープライズ・ネットワーク・ハブないし同等の統合ネットワークアクセスサーバである。

このようなアーキテクチャにおいて、当初のダイアルアップ・サーバ（通信シャシ２０）の場所を、中間ネットワークがダイアルアップ・プロトコル接続（ＰＰＰ）を切断し、トンネリングサーバ３０において目標とするネットワーク２２又は２４にアクセスを与える場所から分離することができる。目標ネットワークとしてのインターネット２２を支援することに付け加えて、このアーキテクチャは仮想個人ネットワークへのアクセスを支援することにより、ワイヤレスユーザに対して、該ユーザの企業又はプライベートネットワーク、例えば図１の企業体ネットワーク２４に確実にアクセスすることを可能にする。

このアーキテクチャにより更に、前記本社（ＣＯ）におけるローカル通信シャシ２０を管理しているインターネットサービスプロバイダは、ＩＳＰクライアントだけでなく、他のインタフェースサービスプロバイダのクライアントに対してもインタフェースアクセスを提供することが可能となる。これは、インターネットサービスプロバイダのバックボーンネットワーク２６に接続された一つ又は複数の認証サーバ３２Ａ，３２Ｂを利用することにより達成される。認証サーバ３２Ａ，３２Ｂは最初のＩＳＰクライアントに対する認証とアクセス許可を実行する。第２のトンネリングサーバ３４は専用線３６（又はＬＡＮないしＷＡＮ）を介して又は直接に第２のＩＳＰのバックボーンネットワーク３８に接続される。この実施例では、認証サーバ３２Ａは通信シャシ２０を運営している第１のＩＳＰ用のクライアントリストを有しており、後述するような様々な簡単な方法を用いて、通信装置２０にダイアルしている遠隔ユーザが、ＩＳＰのバックボーン２６を介してインターネット２２にアクセスすることが許されているかどうかを判

断できる。（当該呼出が第１インターネットサーバプロバイダのクライアントの一人から行われているため）アクセスが認められていれば、当該呼出はネットワーク２２を介してインターネットにルーティングされる。そうでなければ、後述するような他のプロシージャが開始される。

本発明は、遠隔ユーザからの呼出には発信者の電話番号とダイアルされた電話番号を示す情報が含まれていることを利用する。この情報は第１段階の認証機構として使用される。認証サーバ３２Ａがこの第１段階認証を実行し、遠隔ユーザが第１インターネットサーバプロバイダのクライアントでなく（例えば電話番号がクライアント電話番号リストと一致しないため）、第２のインターネットサービスプロバイダのクライアントであると判断された場合、認証サービス３２Ａは認証要求を、第２インターネットサービスプロバイダのバックボーン３８に接続された第２の認証サーバ４０に送り、第１段階認証が行われる。この通信は専用線４２（専用通信回線、ＰＯＴＳ回線等）を認証サーバ３２Ａと、第２のインターネットサーバプロバイダにより運営されている認証サーバ４０との間に設けることにより円滑化される。

認証の結果が肯定であれば、認証サーバ４０は認証サーバ３２Ａに結果を通知し、ワイヤレスユーザ１２はネットワーク２６又はトンネリングサーバ３４を介してインターネット２２に対するアクセスが与えられるか、又は、遠隔ユーザ１２と第２認証サーバ４０の間でオプションとして第２段階のパスワード式の認証が行われる場合もある。

このような特徴の組み合わせにより、通信シャシ２０並びに認証サーバ３２Ａを運営しているＩＳＰ又は

その他の組織に対して、それらがクライアントに提供するサービスを大幅に増加する能力が与えられる。また、この組み合わせにより、ＩＳＰは他のインターネットサービスプロバイダに対してもインターネットアクセスを提供することが可能となり、その過程でそのようなサービスに対する収益がおそらく生ずる。ワイヤレスユーザから見れば、ワイヤレスネットワーク１６を介しての通信装置２０

へのローカル呼出により、インターネット又は企業ネットワークへアクセスできる。

本発明の好適な実施例では、通信シャシ２０は統合汎用コンピュータプラットホームを備えた前述の総合制御ネットワーク企業体ハブ等の強力な通信プラットホーム、すなわち３ＣＯＭ社から入手可能なEdgeServer^{TM}である。この製品を利用することにより、通信シャシは、マイクロソフト社のウィンドウズＮＴ等の市販の独立型オペレーティングシステムや、その他の遠隔アクセスソフトウェア製品、例えばＲＡＤＩＵＳ（Remote Authentication Dial In User Service）を動作させることが可能となる。上述のインターネットアクセス方法では、好適には、課金及び認証機能はＲＡＤＩＵＳプロトコル、又はその他の市販又は公知の課金ソフトウェアプログラムを利用して使用される。ＲＡＤＩＵＳプロトコルは公知のプロトコルであり、本願明細書に参照として引用するＲＦＣ２０５８、１９９

７年１月、に記載されている。

本発明の好適な実施例では、２段階の認証により、インターネット２２又は企業／プライベートネットワーク２４に対するアクセスが、ネットワーク２６を介してのアクセスが認められているワイヤレスユーザに対してのみ与えられる。認証の第１段階は、遠隔ユーザ１２、１４によりダイアルされた番号と、ワイヤレスユーザ１２、１４の発信者の番号（すなわちコンピュータ１２又はＰＤＡ１４に関連付けられたユーザの電話番号）に基づいて行われる。認証の第２段階は、テストユーザ名及びパスワード認証プロトコル（ＰＰＰ及びＴＥＬＬＮＥＴトンネリング用）に基づいて行われるか、又はチャレンジ／レスポンスプロトコル（ＰＰＰトンネリング専用）に基づいて行われる。これらの認証プロシージャの詳細は以下に説明する。

図１において、通信装置２０はまた好適には、通信装置内のインターネットインタフェースから直接の、すなわちトンネリングを介さないインターネット２２へのアクセスも支援する。この機能により、通信装置は両方の認証段階、ＰＰＰプロトコルの切断を行い、インターネットプロトコルトラフィックをルーティン

グする。

本発明の別の実施例では、通信装置２０は移動又は陸上から発信されたデータ呼出に対して直通ＰＳＴＮ（Public Switched Telephone Network）接続を可能に

する。この実施例では、通信シャシ２０、例えば前述のトータル・コントロール・ネットワーク・エンタープライズ・ハブは、必要とされるモデムと電話回線インタフェース及びこれらの機能を実行するための処理回路を含む。この実施例は、インターネットサービスプロトコルが市内の電話会社である場合に特に有利である。本発明によるインターネットアクセス方法によれば、通信装置２０は、移動データユーザから移動発信データ呼出の最中に発せられたＡＴＤコマンド内の被呼出番号を抽出ないし取り出す。ほとんどの呼出番号の場合、通信装置２０は呼出を通常のＰＳＴＮモデム呼出として処理する。しかし、呼出番号がインターネットアクセスに関連付けられている場合、通信シャシ２０は呼び出された番号（ＩＳＰのバックボーンネットワーク２６上、又は通信シャシ２０に専用線３６、４２又はその他のネットワークを介して接続されている）に関連付けられた認証サーバ３２Ａにおいて第１の認証段階を実行する。認証サーバ３２Ａは、認証サーバ３２Ａの管轄下にあるインターネット２２又はネットワーク２４をアクセスすることが遠隔ユーザに許可されているかどうかを判断する。

図２は図１の通信シャシ又はネットワークアクセスサーバ２０の好適な形態を簡略化して示した機能ブロック図である。この通信シャシ又はネットワークアクセスサーバ２０はワイヤレスユーザのみならず、公衆

交換電話ネットワークからダイアルしているユーザにもサービスを提供することができる。そのため、シャシは本発明の実施には必要とされない機能を含み、ＰＳＴＮが可能にされている本発明の特定の実施例において必要とされる別の機能を実行する。図２のネットワークアクセスサーバ２０は基本的に、出願人の譲受人から入手可能な市販製品であるトータル・コントロール・ネットワーク・エンタープライズ・ハブの現行モデルのアーキテクチャと設計を一にする。業界のそ

の他のメーカの統合アクセスサーバを適当に修正して本発明の機能を得ることも可能であり、この明細書に記載された実施例のみに本発明が限定されていると解すべきではない。

ネットワークアクセスサーバ２０は電話ネットワークインタフェースカード５０を含む。この電話ネットワークインタフェースカード５０は、Ｔ１，Ｅ１及びＩＳＤＮ基本レートインタフェース（ＰＲＩ）回線、及びフレームリレー回線等の時分割多重ディジタル電話回線に接続されている。ネットワークインタフェースカードは、無線円滑ユーザからのディジタルデータを、フレームリレー回線ＦＲ上のワイヤレスサービススイッチを介して受け取る。インタフェースカード５０は電話回線を物理的に受け入れるためのコネクタを有する。該カード５０はさらに、入力信号からクロック信号とデータを取り出し、出力及び入力データ流に

多重化及び多重分離を施すＣＳＵを有し、それによって呼出をキャリアの時間スロット内に配置する。カード５０は入力電話信号をＮＩＣ／ＮＡＣ（network interface card/network application card）バス５４を介してＴ１／Ｅ１／ＩＳＤＮ　ＰＲＩ／ネットワークアプリケーションカード５６に送信する。アプリーケーションカード５６は、取り出された電話回線データに対してフレーミングを供給することにより、フレームリレー時分割多重データ、Ｔ１　ＤＳ０チャネルデータ、又はＩＳＤＮ PRI信号に含まれたＩＳＤＮ 2B+Dチャネルデータを取り出し、その後時間／空間スイッチを利用して、チャネルデータを、シャシ内バスミッドプレーン５２の一部である時分割多重バス６０上の時間スロットに切り換える。

入力信号がワイヤレスサービス中央オフィスからのものであり、フレームリレー回線上でサーバに到着したものである場合、チャネルデータは通常モデムにおいて行われる信号変換処理は必要とせず、ＴＤＭバス６０を介してルーティング及びＬＡＮ／ＷＡＮインタフェースカード６２にルーティングされる。トータル・コントロール・エンタープライズ・ネットワーク・ハブでは、このカード６２は“エッジサーバ（EdgeServer）”カードとして公知であり、Ascend社、Livingston社その他のメーカのネットワークアクセス装置も同様のインタフェースを有

している。エッジサーバカ

ード６２は、ＴＣＰ／ＩＰプロトコルに従ってデータパケットを組み入れた一対のミュンヘンチップを有し、ＬＡＮ／ＷＡＮインタフェース又はトータルサーバを介して直接目的地に送信する。

公衆交換電話ネットワークに接続されたユーザから発せられた呼出であり、信号変換が必要な場合、ＴＤＭバス６０は呼出をマルチ・モデム・モジュール内のモデム又はカード６４に向ける。内部シャシバス５２はさらに高速並列パケットバス５８を有し、該バス５８は、復調／信号変換後のデータをエッジサーバカード６２内のルーティングエンジンに伝送するために、カード６４内のモデムをエッジサーバカード６２に接続する。複数のアナログネットワークインタフェースカード６３が、モデムを直列インタフェース６５に接続するために設けられている。

電話回線インタフェースカード５０とアプリーケーションカード５６、モデムカード６３、６４、内部シャシバスコンプレックス５２（ＴＤＭバス６０及び並列バス５８を含む）、並びにエッジサーバカード６２のコンピュータネットワークインタフェース６６は、上述のBaum他の米国特許第５５７７１０５号：「データ通信用の電話呼出交換及びルーティング方法」に、また、Walsh他の米国特許第５５２８５９５号：「モデム入出力信号処理方法」に詳細にそれぞれの構成回路と動作が記載されている。好適な内部シャシバスの詳

細な構造はPanzarella他の米国特許第５４１６７７６号「モデムバックプレーン技術」に開示されている。この特許は３ＣＯＭ社に譲受されており、参照として本明細書に引用する。マネージメントカードによるシャシの運営はPanzarella他の米国特許第５４３６６１４号「モデム管理技術」にも詳細に説明されている。この米国特許もまた３ＣＯＭ社に譲受されており、参照として本願明細書に引用する。

エッジサーバカード６２は汎用計算プラットホーム７０を含み、該プラットホーム７０により市販のスタンドアローン型又はシェアウェアによるオペレーティ

ングシステム（ウィンドウズＮＴ等）が駆動される。カード６２は本願明細書に参照として引用する、Willium Verthein他の特許出願第　　号に詳細に記載されている。

電話回線インタフェース、アプリケーションカード、モデムカード、管理カード（図示しない）、及びカード６２のコンピュータネットワークインタフェース６６は公知の製品内に存在し、又は公知の文献に記載されており、当業者であればそのような回路（ないしは同等物）を如何にして設計・製作するかは明らかであるので、通信アクセスシャシ１０のこれら構成要素の説明は省略する。また、通信シャシ１０のアーキテクチャ又は設計に関する詳細も特に重要でない。

エッジサーバカード６２はＴＤＭインタフェース７

２を有し、該インタフェースはフレームリレーＦＲ回線からＴＤＭバス６０を介してチャネルデータを受け取る。計算プラットホーム７０は市販のＩＢＭ互換機パソコン、それに付随する統合中央処理ユニット７４、及びキーボード、フロッピーディスク、モニタ並びにマウス用の周辺機器インタフェースから構成される。計算プラットホームはまた、内部記憶用ハードディスクドライブ７６を含む。計算プラットホームはさらにパケットアセンブリ・逆アセンブリ回路７８を含み、それによってモデムモジュール６４内のモデムからのデータパケットが、汎用計算プラットホーム７０の使い易いフォーマットに組み立てられる。汎用計算プラットホームはＮＩＣ／ＮＡＣバス接続を介して通常のネットワークインタフェース６６とも通信する。計算プラットホームはまた、第２のＩＳＡバス８２を介して外部記憶拡張バスインタフェース８４とも通信を行う。該インタフェース８４は外部ディスクドライブ又はその他適当な記憶装置に接続され、通信シャーシ２０の記憶容量を増大させるために使用される。好適な実施例では、後述するような通信シャーシ２０内でのトンネリング及び認証機能を駆動するためのソフトウェアは、エッジサーバカード６２内の汎用計算プラットホーム７０内にロードされている。

上述のように、図２の通信シャーシによるアーキテクチャ及び機能は、ワイヤレスネットワーク上の遠隔

ユーザをＩＳＰバックボーン、企業ネットワーク又はインターネットに接続するために通常必要とされる機能以上の機能を提供する。図２Ａはモデムを有しない別の装置の略図である。この装置は、通信装置用のＰＳＴＮ切断機能が設けられていない実施例において用いると好適である。図２Ａの実施例では、回線インタフェースユニット、デマルチプレクス回路及びフレーミング回路を有したフレームリレーインタフェース１００が１つのモジュール内に設けられている。インタフェース１００はチャネルデータをＴＤＭバスコンプレックス内において時間スロット上に配置する。ＴＤＭバスコンプレックス１０２はインタフェース１００をＬＡＮ／ＷＡＮインタフェース１０４に接続する。ＬＡＮ／ＷＡＮインタフェース１０４は好適には一般的なイーサネット又はその他一般のインタフェースから構成される。後者の場合は、呼びルーティング、認証、トンネリングその他本願明細書に記載の機能を実行するソフトウェアがロードされた汎用計算プラットホームにより修整される。

図１、２及び２Ａから、ディジタルデータ源１２をコンピュータネットワーク２４、２２（企業内プライベートネットワーク、インターネット、ワールド・ワイド・ウェブ等）に接続する方法が開示されていることが明らかであろう。ディジタルデータ源１２はディジタルデータを発生し、無線伝送媒体を介して無線サーバキャリアと通信を行う。キャリアはディジタルデータを多重化し、回線ＦＲ等の高速ディジタル電話回線に送る。この方法は以下のステップを有する。

（１）ネットワークアクセスサーバ又は通信シャシ２０においてディジタルデータ受け取り、該ディジタルデータから少なくとも（ａ）ディジタルデータ源１２により呼び出された電話番号、又は（ｂ）ディジタルデータ源と関連付けられた電話番号、を有するネットワークアクセス認証データを抽出する。

（２）認証データを、通信装置２０に接続されたローカルエリア又はワイドエリアコンピュータネットワークを介して、コンピュータネットワーク２４又は２２用のネットワーク認証サーバ３２Ａ又は３２Ｂに送信する。ネットワーク認証サーバはローカルエリア又はワイドエリアコンピュータネットワーク２６を介して通信シャーシ２０と結合されている。

（３）認証サーバ３２Ａにおいて、送信されてきた認証データに基づいて、遠隔ユーザがコンピュータネットワーク２２ないし２４にアクセスすることが許可されているかどうかを判断する。認証サーバ３２Ａは通信シャーシ２０に判断ステップの結果をし、該判断ステップの結果が肯定であるならば、データ源１２に対してコンピュータネットワーク２４へのアクセスを許可する。

この方法はさらに、ローカルエリア又はワイドエリ

アネットワーク２６を介して通信シャーシ２０に結合されたトンネリングサーバ３０又は３４を識別し、ディジタルデータ源１２からのディジタルデータをトンネリングサーバ３０にルーティングしてコンピュータネットワーク２４に対するアクセスを与えるステップを含むことができる。前記通信シャーシ２０はディジタルデータ源１２に対して、コンピュータネットワークへのアクセスを与える。トンネリングサーバの識別は、好適な実施例では、発生した呼び出しから抽出された認証データ（すなわちダイアルされた番号及びダイアルした側の番号）により決定される。この実施例では、認証サーバ３２Ａ又は３２Ｂ内で、通信装置２０とトンネリングサーバ３０間でディジタルデータをトンネリングする際に使用される、データ源１２用トンネリングプロトコルを決定することによっても本発明を実施できる。この決定ステップは例えば、ソフトウェアルックアップテーブル内で、遠隔ユーザ１２（遠隔ユーザ１２の電話番号により識別される）と関連付けられたトンネリングサーバ及び必要なプロトコルを見つけ出すことによっても実行可能である。ディジタル電話はトンネリングサーバを介してトンネリングプロトコルに従ってルーティングされる。本発明の好適な実施例では、ＰＰＴＰ又はＴＥＬＮＥＴプロトコルが使用される。

好適な実施例では、図２の通信シャーシ２０は、T1

/E1ＩＳＤＮインタフェース50/56を介しての公衆交換電話ネットワークに対するアクセスも供給する。通信シャーシ２０は遠隔ユーザ１２からのディジタルデータをそのデータの目的地にルーティングする。このようにして、通信シャーシ２０はコンピュータネットワーク２２と２４に対する直接的ネットワークアクセス

を供給するだけでなく、シャーシ内のモデムを介して信号変調を行い、呼び出しを電話ネットワークを介して遠隔端末、例えば図１のコンピュータ１３に送信可能にする。通信シャーシ２０がどのようにしてＰＳＴＮコネクティビティを与えるかは公知であり、前述のWalsh他の特許に記載されている。

本発明の好適なネットワークアクセス実施例において、第２段階の認証ルーチンにより、遠隔ユーザの指定ネットワークへのアクセスが許可されていることが確認される。これは、PAPやCHAPルーチン等のパスワード認証プロシージャを、（１）トンネリングサーバ３０又は（２）認証サーバ３２Ａと遠隔ユーザの間で実行することにより、又は（３）認証サーバ３２Ａとトンネリングサーバ３０／３４間で実行することにより、第２レベルの認証を行うことにより達成される。これらのルーチンはいずれも公知である。

本発明の１つの実施例においては、高速電話回線を介してユーザ１２から電話呼び出しを受け取るよう構成されたネットワークアクセスサーバ又は通信シャーシ２０を有したインターネットサービスプロバイダによる使用に適したインターネットアクセス方法が開示される。この方法は以下のステップを有する。

（１）ネットワークアクセスサーバ２０を、ローカル又はワイドエリアネットワーク２６を介して認証サーバ（３２Ａ又は３２Ｂ等）に接続する。

（２）ユーザ１２により発生された呼び出しから、少なくとも（ａ）ユーザの呼び出した電話番号、又は

（ｂ）ユーザと関連付けられた電話番号、を含むネットワークアクセス認証データを抽出する。

（３）発生呼び出しから抽出したネットワーク認証データを認証サーバ３２Ａ又は３２Ｂにルーティングし、ネットワークアクセス認証データに基づいてユーザを認証する。

（４）ネットワークアクセスをユーザに与えるためのトンネリングサーバ（例えば３４）を識別し、通信シャーシ２０に該トンネリングサーバを通知する。

（５）通信シャーシ２０からのディジタルデータをトンネリングサーバ３４にトンネリングする。

（６）前記ディジタルデータを前記トンネリングサーバによりインターネットに送る。

好適な実施例では、この方法は、トンネリングステップのためにユーザに対するトンネリングプロトコルを識別するプロセスにより達成される。例えば、認証サーバ３２Ａ又は３２Ｂ又は４０により、遠隔ユーザ

の特徴、指定されたトンネリングサーバの必要とする条件、その他に従って、ユーザを特定のトンネリングプロトコル（ＰＰＴＰ又はＴＥＬＮＥＴ）に関連付けることができる。そのような情報は典型的には認証サーバ３２Ａのメモリ内に記憶されている。

さらに、本発明はインターネットサービスプロバイダシステムを無線インターネットユーザとして想定している。このインターネットサービスプロバイダはネットワークアクセスサーバ２０（図２）を有し、該サーバは以下の構成要素を有している。

（１）無線インターネットユーザからの呼出を受ける高速ディジタル電話回線ＦＲインタフェースと、前記無線インターネットユーザに関連付けられたディジタルデータをインターネットに送出するためのインターネットゲートウェイ（図２のＷＡＮインタフェース６６等）。

（２）通信媒体２６を介してネットワークアクセスサーバ２０に結合されたインターネットアクセス認証サーバ（３２Ａ等）。該認証サーバは無線インターネットユーザに関連付けられたディジタルデータから抽出されたインターネットアクセス認証データに応じて動作する。

（３）認証サーバ３２Ａはさらに、インターネットアクセス認証データに基づいて、無線インターネットユーザ１２がインターネットにアクセスすることが許

可されているかどうかを判断するためのメモリを備える。インターネット認証サーバは認証応答をネットワークアクセスサーバ２０に送出する。ネットワークアクセスサーバ２０は認証サーバからの認証応答に応じて、無線インターネットユーザに対してインターネットへのアクセスを認めるか、又は該無線インターネッ

トユーザからの呼出に関してその他の何らかの動作を行う。例えば、インターネットサービスプロバイダは認証照会を、第２のインターネットサービスプロバイダにより運営されている他の認証サーバ（図１の４０等）に転送し、前記ユーザが第２のインターネットサービスプロバイダのクライアントであるかどうかを確かめる。

本発明の好適な実施例の実施の詳細に関しては、図３～１１を参照して説明する。

図３は遠隔ユーザ１２、通信シャシ２０、インターネットサービスプロバイダバックボーンネットワーク２６内のルータ（図示しない）、及び図１の指定されたトンネリングサーバ３０又は３４間のトンネルインタフェースのプロトコルスタックとアーキテクチャを図示したものである。図３では、番号Ｌ１とＬ２は下位プロトコル（データリンク層等）を示している。ＩＰはインターネットプロトコルを示す。ＰＰＰはポイントツーポイントプロトコルを示す。ＴＣＰは伝送制御プロトコルを示す。非同期（Async）という用語は遠隔

ユーザ１２と関連付けることのできる非同期プロトコルを示し、ＴＥＬＮＥＴプロトコルは通信シャシ２０とトンネリングサーバ内で非同期通信のために用いられる。図から明らかなように、通信シャシ２０がトンネリングサーバと通信する際には、ＩＰ及び下位プロトコル上で動作するＰＰＴＰ又はＴＥＬＮＥＴを使用する。

図４に示すように、通信シャシ２０の通信相手である認証サーバ（３２Ａ等）はＲＡＤＩＵＳを実行し、ＵＤＰ/ＩＰプロトコルスタックを介して認証と課金を行う。図４は、ネットワークアクセスサーバ又は通信シャシ２０と図１の認証サーバ３２Ａ間の認証・課金インタフェース用のプロトコルを示す。ＵＤＰは、インターネットプロトコル（ＩＰ）の上位に位置するコネクションレス型プロトコルである。

通信シャシ２ーがインターネット２２と通信する場合、トンネリングプロトコルはない。図５に示されているのは、遠隔ダイアルユーザと、該ユーザを目的地端末装置に接続するルータ間の非トンネルインタフェース用プロトコルスタック

である。

図６は、本発明の好適な実施例における呼び出し受入シナリオにおけるＰＰＴＰプロトコルトンネリングの呼出フローを示す。図６では、プロセスは素００における呼出の発生から始まる。呼出は特定の目的地電話番号（図示の例では1-800-123-4567）に関連付けられ

ている。

ステップ１０２では、通信シャシが、ローカルエリアネットワークを介して通信シャシに接続されている認証サーバ（３２Ａ又は３２Ｂ等）に対して第１段階の認証アクセスルーチンを開始する。この認証要求は認証サーバに転送されるソフトウェア構造であり、以下の情報のためのフィールドを含む。（１）遠隔ユーザに関連付けられた電話番号（これは公知の呼出人識別技術又は前記Baum他の特許に記載の方法に従って検知される）；（２）公知の方法により取り出されるダイアルされた電話番号；（３）通信シャシ２０内の呼出に関連付けられた特定のチャネルないしポート番号すなわちポートＩＤ；及び（４）通信シャシ２０のＩＰアドレス。

ステップ１０４では、認証サーバ３２Ａは通信シャシ２０にアクセス応答メッセージを送る。ユーザが、認証サーバ３２Ａの管轄下にあるネットワークに対してアクセス許可されていれば、前記メッセージは、ＰＰＴＰが適切なトンネリングプロトコルであるという確認と、トンネリングサーバのＩＰアドレスの確認と、呼出を受けるトンネリングサーバのポート番号を含む。遠隔ユーザがアクセス許可されていない場合、以下に説明するような図８のプロシージャが使用される。

ステップ１０６では、通信シャシ２０は発生呼出要

求（Incoming-Call-Request）メッセージをトンネリングサーバ３４に送出する。このメッセージは遠隔ユーザのダイアル番号の識別、ダイアルされた電話番号、及びサブアドレスを含む。ステップ１０８では、トンネリングサーバ３４が呼出を受入可能であれば、発生呼出応答（Incoming-Call-Reply）メッセージ、例

えばアクセス照会の結果が肯定であれば「コネクト」を送出する。トンネリングサーバが呼出を受け取れない場合は、図９のプロシージャが使用される。

ステップ１１０では、トンネリングサーバ３４から「コネクト」メッセージが受け取られた場合、通信シャシ２０は呼出受入メッセージをフレームリレー回線ＦＲ及びワイヤレスネットワークを介して遠隔ユーザに送出する。そして入力呼出接続メッセージがステップ１１２において通信シャシ２０からトンネリングサーバ３４に中継される。

ステップ１１４では、好適には（つまりオプションとして）第２段階の認証プロシージャが実施される。ステップ１１６、１１８、１２０、１２２、１２４及び１２６は図６から自明であり、公知のPAP及びCHAPパスワード認証プロトコルの一部であり、当業者には明らかである。

ステップ１２８では、仮にパスワード認証を通過したとして、トンネリングサーバ３４から遠隔ユーザ１２に対して、通信シャシ２０を介して遠隔ユーザ１２とトンネリングサーバ３４間にＰＰＰリンクが確立された旨のメッセージが送られる。この時点で、遠隔ユーザとネットワーク２２又は２４上のホスト間での、インターネットプロトコルに従ったデータパケットの伝送が完了する。

図７は本発明の好適な実施例における、呼出受入シナリオのためのＴＥＬＮＥＴプロトコルトンネリングの呼出フローを示す。このプロセスは概して図６に記載されたものと同様であり、図から自明である。ＴＥＬＮＥＴセッションの確立の為には、通信シャシ２０とトンネリングサーバ３４間におけるハンドシェーキング及びパラメタ折衝が必要である。これは、ステップ１３０及び１３２に示されている。PAP等のログインプロトコルを使用した、認証の第２段階が図示のように実行される。トンネリングサーバ３４からダイアルユーザ１２に対してログイン受入メッセージが送られると、通信サーバ２０とトンネリングサーバ３４を介して、遠隔ユーザ１２とコンピュータネットワーク（インターネット等）上のホスト間で非同期伝送が実行される。

アクセス認証の第１段階で、認証サーバが、該認証サーバの管轄下にある指定されたネットワークへのアクセスが遠隔ユーザに許可されていない（例えば、遠

隔ユーザの電話番号が、シャシ２０を運営しているインターネットサービスプロバイダのインターネットク

ライアントデータベースに合致しないため）と判断することもある。このシナリオに対処する好適な方法が図８に示されている。すなわち図８は認証失敗シナリオにおける呼出フローを示す。認証サーバ３２Ａが、遠隔ユーザが許可されていないと判断すれば、認証サーバ３２から通信シャシ２０に対してアクセス拒否メッセージが送られる。このメッセージは、アクセス拒否の理由を示したフィールドを含むことができる。そのような理由は例えばダイアルした電話番号が間違っている、ISPがユーザの電話番号を認識しない、ユーザの毎月の使用料の支払いが遅れている、認証サーバが使用中止になっている、等である。通信シャシ２０はその場合、遠隔ユーザ１２に対して後ほどトライし直すようメッセージを送るか、該呼出をＰＳＴＮ／モデム呼出として扱い呼出をＰＳＴＮシステム上でルーティングするか、又は該呼出を拒絶して切断シーケンスを開始する。

さらには認証サーバ３２Ａがネットワークへのアクセスを許可するが、トンネリングサーバ３０又は３４が遠隔ユーザ１２と目標ネットワーク２２ないし２４間でのデータ転送のための機構として機能出来ないという状況が考えられる。図９はトンネリングサーバアクセス拒絶シナリオにおける呼出フローを示す。第１ステップ１００、１０２、１０４及び１０６は図６と共通である。トンネリングサーバ３４が呼出を処理で

きない場合、トンネリングサーバ３０ないし３４は通信シャシ２０に、入力呼出応答を、呼出を受け入れられない旨のメッセージないしフィールドと共に送る。この時点で、通信シャシ２０は遠隔ユーザ１２に対して後ほどトライし直す旨のメッセージを送るか、該呼出をＰＳＴＮ／モデム呼出として扱い電話システム上でルーティングするか、又は単に呼び出しを拒絶する。

前記図６と７に関連して説明した認証の第２段階において、ユーザがパスワード認証プロシージャにおいて失敗することもある。図１０はＰＰＴＰプロトコルにおける認証失敗シナリオにおける呼出フローを示す。ＰＰＴＰプロトコルでは

、ログインパスワード認証プロシージャが、ネットワークアクセス認証プロシージャの第２段階として実行される。ステップ１４０では、アクセス拒絶メッセージが認証サーバ３２Ａからトンネリングサーバ３０／３４に対して送出される。この時点（ステップ１４２）で、トンネリングサーバはログイン拒絶メッセージを遠隔ユーザ１２に送る。

図１１は、ログインパスワード認証プロシージャが、ネットワークアクセス認証プロシージャの第２段階として実行される、ＴＥＬＮＥＴ用認証失敗シナリオにおける呼出フローを示す。このプロセスは基本的に前記のプロセスと同様に進行する。

ＰＰＴＰ及びＴＥＬＮＥＴトンネリング、課金及び

第１・第２という２段階の認証の好適な実施例を以下に詳細に説明する。

プロトコルインタフェース

通信シャシ２０はダイアルユーザ（無線端末）、ＭＳＣ，ルータ、認証サーバ、及びトンネリングサーバとインタフェースする。本明細書では認証サーバとトンネリングサーバに対する通信シャシインタフェースについてのみ説明する。その他のインタフェースは当業者には明らかである。

ＰＰＴＰトンネリング

ＰＰＴＰトンネリングは、認証の第１段階中のＲＡＤＩＵＳ　アクセス応答メッセージからのログインサービス属性に基づいて使用可能にされる。プロトコルがＰＰＴＰ値（ＲＦＣ２０５８ではＴＢＤ）を有していれば、ＰＰＴＰトンネリングが通信シャシとトンネリングサーバ間に設定され、呼出人からの以後のトラフィックがトンネルされる。

通信シャシゲートウェイはＰＰＴＰ　ＲＦＣ内のＰＡＣ（ＰＰＴＰアクセスコンセントレータ）と同等であり、トンネリングサーバはＰＰＴＰ　ＲＦＣ内のＰＮＳ（ＰＰＴＰネットワークサーバ）と同等である。以下のＰＰＴＰの説明では、ＰＡＣ及びＰＮＳという用語を使用する。

個々の構成されたＰＰＴＰ　ＰＡＣ-ＰＮＳ対に関して、ＰＡＣ（通信シャシ）とＰＮＳ（トンネリングサ

ーバ）間のインタフェースは２つの並列要素から構成される。すなわち、

１．ＴＣＰ上で動作する制御接続

２．個々の対間のユーザセッションのためのカプセル化されたＰＰＰパケットを伝送するＩＰトンネル。

ＰＰＴＰ制御接続

ＰＡＣとＰＮＳ間でＰＰＰトンネリングを生じさせる前に、それらの間で制御接続が確立される必要がある。制御接続は標準的なＴＣＰセッションであり、その上をＰＰＴＰ呼出制御及び管理情報が通過する。制御セッションはＰＰＴＰトンネルを介してトンネリングされているセッションと論理的に関連付けられてはいるが、別個のセッションである。

ＰＰＴＰトンネル接続

ＰＰＴＰはそれぞれの通信しているＰＡＣ-ＰＮＳ対においてトンネルを確立することを必要とする。トンネルはＰＡＣ-ＰＮＳ対に関わるセッションのための全てのユーザセッションＰＰＰパケットを伝送するために使用される。ＧＲＥヘッダ内にあるキーにより、どのセッションに特定のＰＰＰパケットが属するかを示す。このようにして、ＰＰＰパケットは所与のＰＡＣ-ＰＮＳ対間の単一のトンネル上で多重化及び逆多重化される。キーフィールドにおいて使用する値は

、制御接続上で実行される呼び出し確立プロシージャによって確立される。

ＰＰＴＰ制御接続メッセージ

制御接続管理メッセージ：

以下のメッセージから構成される。

・制御接続開始要求

・制御接続開始応答

・制御接続停止要求

・制御接続停止応答

・エコー要求

・エコー応答

呼び管理メッセージ：

以下のメッセージから構成される。

・出力呼び要求（この時点ではサポート無し）

・出力呼び応答（この時点ではサポート無し）

・入力呼び要求

・入力呼び応答

・入力呼び接続完了

・呼びクリア要求

・呼び切断通知

エラー報告

・ＷＡＮエラー通知

ＰＰＰセッション制御

・セットリンク情報

ＰＰＴＰトンネル接続メッセージ

ＰＰＴＰデータＰＤＵ：

ＰＰＰフレームはそれぞれＧＲＥ（Generic Routing Encapsulation Header；汎用ルーティングカプセル化ヘッダ）内でカプセル化されている。ＧＲＥは参照として本願明細書に引用するコメント要求（ＲＦＣ１７０１、１９９４年１０月）に記載されている。

Ｔｅｌｎｅｔ　トンネリング

ＰＰＴＰとＬ２ＴＰプロトコルは非同期トラフィックをトンネリングするようには設計されていない。同期トラフィックはＴｅｌｎｅｔプロトコル（ＲＦＣ８５４を参照）によりトンネリングされる。

Ｔｅｌｎｅｔの実施はＥＣＨＯ，linemode、binary、SUPPRESS GO AHEAD等のＴｅｌｎｅｔコマンド及びオプションを支援しなければならない。トンネリングサーバは任意のＴｅｌｎｅｔセッションにおいてＴｅｌｎｅｔ接続の最中に１つのモードから別のモードへ切換を要求出来なければならない。この切換は例えばＥＣＨＯからＮＯ ＥＣＨＯ、linemodeを経てbinary伝送へという具合である。

さらに、通信シャシゲートウェ

イにおいてはエスケープ機能を使用禁止にして、ダイアルユーザが通信シャシゲートウェイ上のローカルモードに入ることを防止する必要がある。

Ｔｅｌｎｅｔトンネリングは、第１段階認証中に、ＲＡＤＩＵＳアクセス応答メッセージからのログインサービス特性に基づいて使用可能にされる。ログインサービス属性が値Ｔｅｌｎｅｔを有していれば、通信シャシとトンネリングサーバ間にＴｅｌｎｅｔが設定され、発呼者からの以後のトラフィックがトンネリングされる。

ＲＡＤＩＵＳ認証インタフェース

２段階の認証が使用される。認証の第１段階は発呼者番号、被呼番号、及び通信シャシＩＰアドレスに基づいて行われる。認証の第２段階は、ユーザ名、パスワード、及び／又は呼び掛け・応答（オプション）に基づいて行われる。

ここでは第１と第２段階両方のＲＡＤＩＵＳ認証のやりとりを説明する。トンネリングオプションの何れか１つを使用する場合、エンドユーザ認証は、通信シャシに対して透過性（transparent）である認証の第２段階においてトンネリングサーバにより行われる。非トンネリングインターネットアクセスの場合、通信シャシは認証の両方の段階を行う（第１段階は省くこともオプションとして可能である）。

以下の一般的動作がＲＡＤＩＵＳインタフェースに該当する。

１．この文書はＩＥＴＦ ＲＡＤＩＵＳ認証ＲＦＣ２０５８に従っている。認証サーバはＲＦＣに規定されたＲＡＤＩＵＳサーバ機能を供給する。通信シャシ及びトンネリングサーバはＲＡＤＩＵＳクライアント機能を実施する。

２．通信シャシは少なくとも２つの認証サーバを個々の特別インターネットアクセス被呼番号に関連付けることができるものとする。これら２つ（又はそれ以上）の認証サーバは第１及び第２のＲＡＤＩＵＳ認証サーバ機能を供給する。それぞれの認証サーバは構成可能なサーバＩＰアドレス及びＵＤＰポートにより識別可能である。複数のインターネットアクセス被呼番号が認証サーバを共有する場合もあるし、そうでない場合もある。

３．ＲＡＤＩＵＳ共有秘密（１～１５文字）はサーバ毎に行政的に構成される

。この明細書では共有された秘密が通信シャシゲートウェイとＲＡＤＩＵＳノード（認証サーバ）間でどのように管理されるかは論じないが、そのような詳細は当業者には明らかである。

４．通信シャシゲートウェイは再送信アルゴリズムを実施し、それによってアクセス要求の消失に対処できる。構成可能な再送信カウンタは、特定のインターネットアクセス呼出番号に対する認証サーバがいつ動

作停止中であるかを判断し、停止中は通信シャシはオプションとして、標準的なＰＳＴＮ／モデムアクセスプロシージャに従う。

認証インタフェース第１段階

アクセス要求メッセージ：

ＲＡＤＩＵＳアクセス要求メッセージは通信シャシ２０によりＲＡＤＩＵＳサーバ（認証サーバ３２Ａ）に送られ、入力呼出が示される。以下は、メッセージと共に送られる属性のリストである。

・ユーザ名：全ての入力呼出に対してＶＥＮＤＯＲＩＤに設定。

・ユーザパスワード：ゼロに設定。

・ＮＡＳ-ＩＰアドレス：通信シャシのＩＰアドレスに設定。

・ＮＡＳポート：通信シャシ上の発呼者に関連付けることのできるポート番号又はその他の識別子

・被呼局ＩＤ：被呼者の番号又は電話識別子。これは発呼者の希望するサービスを識別するために使用される。

・発呼局ＩＤ：発呼者の番号又は電話識別子。これは認証第１段階に使用することもできる。

・ＮＡＳポートタイプ：通信シャシスイッチ上でユーザにより使用されるポートの種類を特定する。（ＲＦＣ２０５８における無線アクセス用ＴＢＤ値）

アクセス受入メッセージ

ＲＡＤＩＵＳアクセス受入メッセージはＲＡＤＩＵＳ（認証サーバ）により通信シャシ２０に送られ、特定のサービスに対する入力呼出の受入が示される。以

下は、認証サーバから通信シャシに送られる属性のリストである。

・サービスタイプ：ＰＰＴＰ又はＴｅｌｎｅｔトンネリングに対しては１（ログイン）に設定。ＰＰＰを使用する非トンネリングインターネットアクセスに対しては２（フレーム化）に設定。

・ログインサービス：０－Ｔｅｌｎｅｔ又はＴＢＤ－ＰＰＴＰに設定。サービスタイプ属性が２（フレーム化）に設定されている場合は使用されない属性。

・ログインＩＰホスト：発呼者が接続されるべきトンネリングサーバのＩＰアドレス。サービスタイプ属性が２（フレーム化）に設定されている場合、使用されない属性。

・ログインＴＣＰポート：発呼者が接続されるべきトンネリングサーバ上のＴＣＰポート。サービスタイプが２（フレーム化）に設定されていれば使用されない属性。

・応答メッセージ：Ｔｅｌｎｅｔユーザに対してのみ送られるオプション。通信シャシはこの属性を非同期ストリングとして、トンネリングサービスに対するＴ

ＥＬＮＥＴトンネリングを完了する前に転送する必要がある。

・フレーム化プロトコル：サービスタイプ属性が２（フレーム化）に設定されていれば、１に設定される。サービスタイプが１（ログイン）に設定されていれば使用されない属性。

アクセス拒絶メッセージ

ＲＡＤＩＵＳアクセス拒絶メッセージはＲＡＤＩＵＳにより通信シャシに送られ、特定のサービスに対する入力呼出を否定する。通信シャシはこのメッセージを受け取ると、通常のＰＳＴＮ／モデムプロシージャに進む。応答メッセージ属性がアクセス拒絶メッセージに含まれていれば、通信シャシはＡＳＣＩＩストリングメッセージをユーザに送る。以下の属性はオプションとしてＲＡＤＩＵＳから通信シャシに送ることができる。

・応答メッセージ：Ｔｅｌｎｅｔユーザのみに送られるオプション。通信シャシは、通常のＰＳＴＮ／モデムプロシージャに進行する前に、この属性の内容を

非同期ストリングとして発呼者に送る必要がある。

第２段階認証インタフェース

ここでは通信シャシと、非トンネリングインターネットアクセスオプションを使用した認証サーバ間の第

２段階認証メッセージを特定する。さらに、トンネリングサーバ（ＲＡＤＩＵＳクライアント）と認証サーバ（ＲＡＤＩＵＳサーバ）間の、何れかのトンネリングオプションに基づいた、考えられる第２段階認証のやりとりの例を説明する。

アクセス要求メッセージ

ＲＡＤＩＵＳアクセス要求メッセージは通信シャシからＲＡＤＩＵＳに送られ、入力呼出が示される。以下のリストはメッセージと共に送られる属性である。

・ユーザ名：この属性は認証を希望しているダイアルインユーザの名前を示す。

・ユーザパスワード：この属性は認証を希望しているダイアルインユーザのパスワード、又はアクセスチャレンジ後のユーザの入力を示す。

・ＮＡＳ－ＩＰアドレス：通信シャシのＩＰアドレスに設定。

・ＮＡＳ－Ｐｏｒｔ：通信シャシ上で発呼者と関連付けることのできるポート番号ないしはその他の識別子。

・サービスタイプ：２に設定（フレーム化）。

・フレーム化プロトコル：１に設定（ＰＰＰ）

・フレーム化ＩＰアドレス：ダイアルインユーザ１２はオプションとしてローカルスタチック構成ＩＰアドレスを要求できる。このＩＰアドレスは、アクセス

受入メッセージ内に含まれた同様の属性により書き換えることができる。

アクセス受入メッセージ

ＲＡＤＩＵＳ受入メッセージはＲＡＤＩＵＳにより通信シャシに送られ、特定のサービスに対する入力呼出の受入が示される。ダイアルユーザはまた、このメッセージによりＩＰアドレスを割り当てられる。以下の属性はＲＡＤＩＵＳから通信シャシに送られる。

・フレーム化ＩＰアドレス：この属性は、ユーザに割り当てるＩＰアドレスを示す。

アクセス拒絶メッセージ

ＲＡＤＩＵＳアクセス拒絶メッセージはＲＡＤＩＵＳ（認証サーバ）により通信シャシに送られ、入力呼出に対して特定のサービスが拒絶される。通信シャシはこのメッセージを受け取ると、要求されたサービスが利用不可能であることを示し、ユーザ接続を切断する。

アクセスチャレンジメッセージ

ＲＡＤＩＵＳアクセスチャレンジメッセージはオプションとしてＲＡＤＩＵＳにより通信シャシに送られ、チャレンジ／レスポンス認証プロシージャをＲＦＣ2058に従って実行する。

ＲＡＤＩＵＳ課金インタフェース

通信シャシとトンネリングサーバの両方は、ＲＦＣ２０５９に規定されたようにＲＡＤＩＵＳ課金クライアント機能を実施する。課金サーバが、呼出を制御する認証サーバと関連付けられていれば、それぞれのＲＡＤＩＵＳ課金クライアントは以下のＲＡＤＩＵＳ課金メッセージをここに記載のように送出する。

通信シャシ及びトンネリングサーバからの課金クライアントは、ＲＡＤＩＵＳ認証サーバからアクセス受入メッセージを受け取ると、課金スタートメッセージを送る。

呼出が一旦放棄、クリア、ないし切断されると、課金クライアントは課金ストップメッセージをＲＡＤＩＵＳ　課金サーバに送る。

課金スタートメッセージはＲＡＤＩＵＳ課金要求により、課金ステータス値を１に設定されて、送信される。課金ストップメッセージはＲＡＤＩＵＳ課金要求メッセージにより、課金ステータスタイプ値を２に設定されて送信される。

課金要求メッセージ

課金要求パケットはクライアントからＲＡＤＩＵＳ課金サーバに送られ、ユーザに対して供給されたサービスに対する課金を供給するための情報を伝送する。

以下は、メッセージと共に送ることのできる課金関連属性の一部である。

・課金ステータスタイプ：この属性は、この課金要求がユーザサービスの始まり（スタート）なのか、又は終わり（ストップ）なのかを示す。

・課金遅延時間：このお属性は、クライアントが何秒間この記録を送ろうとしていたかを示す。この属性をサーバへの到着時間から抽出することにより、課金要求を発生しているイベントのおよその時間を知ることができる。

・課金入力オクテット：この属性は、このサービスが供給されてからいくつのオクテットがポートから受け取られたかを示し、課金ステータスタイプがストップに設定されている課金要求記録内にのみ存在する。

・課金出力オクテット：この属性はこのサービスを供給し始めてからいくつのオクテットが通信シャシに送られたかを示し、課金ステータスタイプがストップに設定されている課金要求記録内にのみ存在する。

・課金セッションＩＤ：この属性は、個別の課金ＩＤであり、ログファイルにおいてスタートとストップ記録のマッチングを容易にする。任意のスタート・ストップ記録は同一の課金セッションＩＤを有していなければならない。課金セッションＩＤはプリント可能なＡＳＣＩＩストリングであることが推奨される。

・課金認証：この属性は、課金要求に含めることが

できき、ユーザがいかに認証されたか、すなわちＲＡＤＩＵＳによってか、送り出し側によってか、又はその他のリモート認証プロトコルによってかを示す。認証なしにサービスを供給されたユーザは課金記録を発生しないはずである。

・課金セッション時間：この属性は、ユーザが何秒間サービスを受け取ったかを示し、課金ステータスタイプがストップに設定されている課金要求記録においてのみ存在し得る。

・課金入力パケット：この属性はフレーム化ユーザに対してサービスが供給されて以来ポートから何個のパケットが受け取られたかを示し、課金ステータスタイプがストップに設定されている課金要求記録においてのみ存在し得る。

・課金出力パケット：この属性はフレーム化ユーザに対してサービスが供給されて以来ポートに対して何個のパケットが送らたかを示し、課金ステータスタイ

プがストップに設定されている課金要求記録においてのみ存在し得る。

・課金中止原因：この属性は、セッションがどのように中止されたかを示し、課金ステータスタイプがストップに設定されている課金要求記録においてのみ存在し得る。

課金応答メッセージ

課金要求を受け取ると、ＲＡＤＩＵＳ課金サーバは課金応答メッセージにより、課金パケットの記録に成功したかどうかに関して応答しなければならない。課金パケットの記録に失敗した場合は送信しない。

グロッサリー

用語及び略語

ＣＤＭＡ（Code Division Multiple Acces；符号分割多重接続）

移動電話及びＰＣＳスペクトラムにおけるディジタル音声及びデータワイヤレス通信のための北米基準。ユーザを無線インタフェース上で多重化するための技術。

インターネットプロトコル（ＩＰ）

ユーザデータグラムをインターネットを介して不信頼性・コネクションレス伝送するための仕組みを定義する。

ＩＷＰ－ＩＰ

通信シャシは、ＴＤＭＡないしＣＤＭＡ移動電話に接続された端末装置と、ＰＳＴＮ及びインターネットネットワークに接続された端末装置とを協働させるための機能を供給する。

第２レイヤトンネリングプロトコル（Ｌ２ＴＰ）

ＰＰＰのリンクレイヤプロトコルのトンネリングを可能にするために定義されたプロトコル。現在のところ草稿ＲＦＣ段階であるが、標準として採用される見通しである。

移動交換センタ（ＭＳＣ）

移動電話又はＰＣＳワイヤレス遠隔通信ネットワーク内のネットワーク要素で

あり、ワイヤレスユーザに対してＰＳＴＮコネクティビティ、制御機能、及び交換機能を提供する。

ＰＰＴＰアクセスコンセントレータ（ＰＡＣ）

外部コネクティビティ（典型的には１つかそれ以上のＰＳＴＮ又はＩＳＤＮ回線を介して）を供給する装置。ＰＰＰ動作及びＰＰＴＰプロトコルを取り扱うことができる。ＰＡＣはＩＰを使用してユーザトラフィックを１つないし複数のＰＨＳにトンネリングする。非ＩＰプロトコルをトンネリングする場合もある。

ＰＰＴＰネットワークサーバ（ＰＮＳ）

汎用計算／サーバプラットホーム上で動作するよう設計された通信シャシ。ＰＰＴＰプロトコルのサーバ側を取り扱う。ＰＰＴＰが完全にＩＰに依存し、インタフェースハードウェアからは独立しているため、ＰＮＳはＬＡＮ、ＷＡＮ装置を含むどのようなＩＰイン

タフェースハードウェアの組み合わせも使用することができる。

ポイントツーポイントトンネリングプロトコル（ＰＰＴＰ）

ＰＡＣとＰＮＳ間のＰＰＰトラヒックをトンネリングするために定義されたプロトコル。ＧＲＥ（Generic Routing Encapsulation；汎用ルーティングカプセル化）機構を使用して、ＰＰＰパケットを伝送するためのフロー・輻輳制御カプセル化データグラムサービスを供給する。「トンネル」制御及び機能管理も支援し、制御接続の設定・解除、及びデータ接続の設定・解除を行う。ＰＡＣとＰＮＳのそれぞれの対に対して１つの制御接続と１つのデータ接続がある。

公衆交換電話回線網（ＰＳＴＮ）

今日、３ＫＨｚ回線音声サーバを世界中の固定終点に供給する、陸上遠隔通信インフラストラクチャ。

リモート認証ダイアルインユーザサービス（ＲＡＤＩＵＳ）

ユーザ接続要求を受入れ、ユーザ認証を行い、クライアントがサービスをユーザに送るために必要な全ての構成情報を返送する。ＲＡＤＩＵＳサービスは他のＲＡＤＩＵＳサーバ又は他の種類の認証サーバに対して

プロキシクライアントとしての役割を果たすことができる。ＲＡＤＩＵＳサーバはＰＰＰ　ＰＡＰ、ＣＨＡＰ，ＵＮＩＸログイン、及びその他の認証機構を支援する。

ＴＥＬＮＥＴ

ＴｅｌｎｅｔはＴＣＰ/ＩＰ接続を介しての２つのネットワーク仮想端末（ＮＶＴ）間の非同期通信を支援するよう設計されている。ＮＶＴは、接続の両者すなわちクライアントとサーバがそれらの実際の出力及び入力端末をマップする仮想の装置である。

時分割多重アクセス（ＴＤＭＡ）

携帯電話及びＰＣＳスペクトルでのデータワイヤレス遠隔通信のための北米基準。無線インタフェース上でユーザを多重化する技術。

伝送制御プロトコル（ＴＣＰ）

ＩＰネットワーク上におけるユーザデータの高信頼度コネクション型伝送機構。

ＴＳ－ＩＰ

トンネリングサーバＩＰアドレス

ユーザデータグラムプロトコル（ＵＤＰ）

ＩＰ上に構築されたコネクションレス型プロトコル。サービスアクセス（ＳＡＰ）はＵＤＰポートとＩＰアドレスにより識別される。

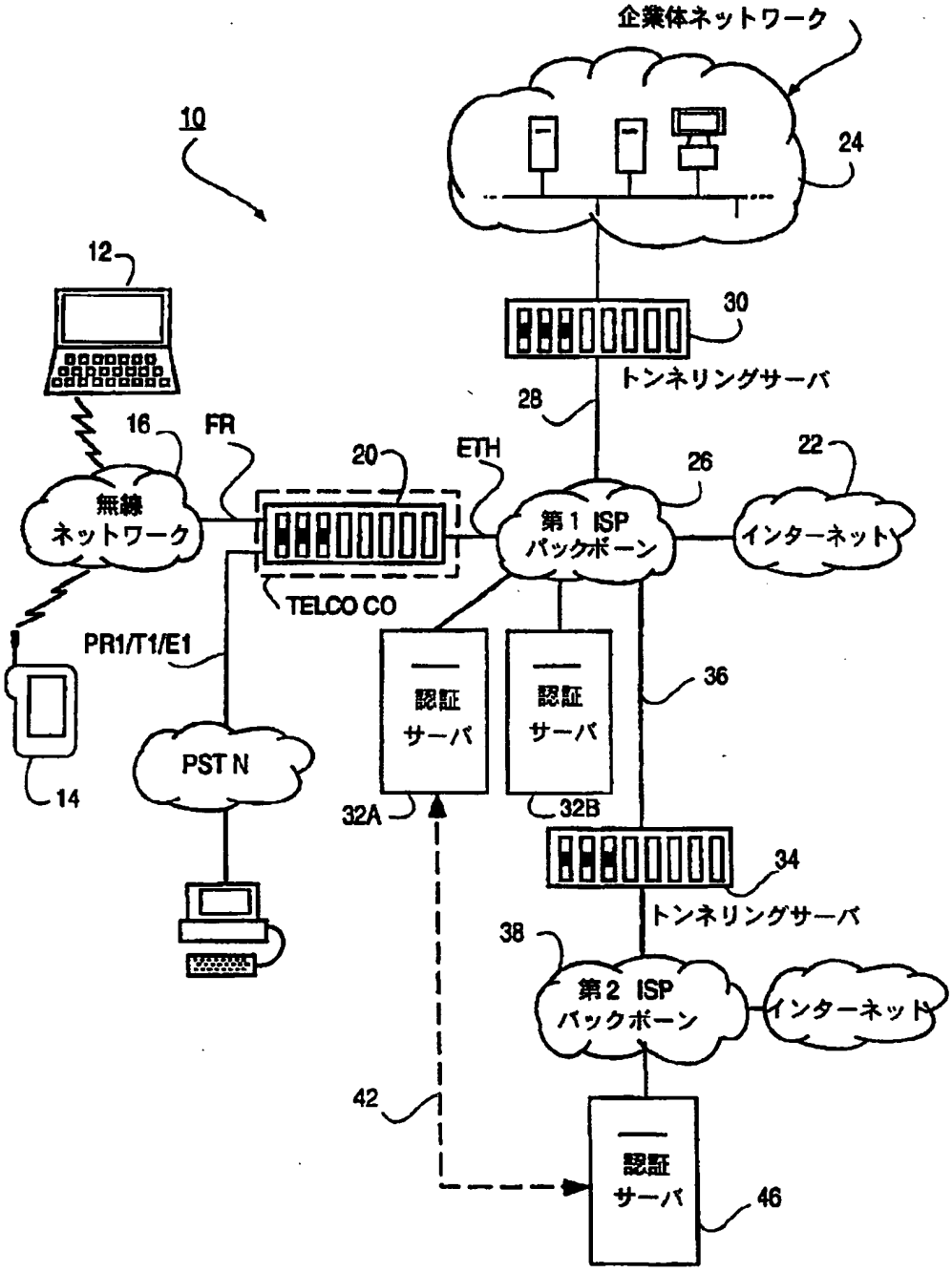
仮想プライベートネットワーク（ＶＰＮ）

安全な情報アクセスを送るためのインターネット上に築かれた安全なネットワーク。

ここに開示した実施例に対しては、本発明の意図および範囲から逸脱することなく様々な変更ないし変形が可能であることが当業者には明らかである。この発明の精神並びに範囲は請求の範囲に記載の通りであり、該記載は上述の詳細な説明に照らして解釈されるものである。

【図１】

FIG. 1


企業体ネットワーク
10
24
12
30
トンネリングサーバ
28
16
FR
20
ETH
26
22
無線
ネットワーク
第１ ISP
バックボーン
インターネット
TELCO CO
PR1/T1/E1
認証
サーバ
認証
サーバ
36
PST N
14
32A
32B
34
トンネリングサーバ
38
第２ ISP
バックボーン
インターネット
42
認証
サーバ
46

【図２】

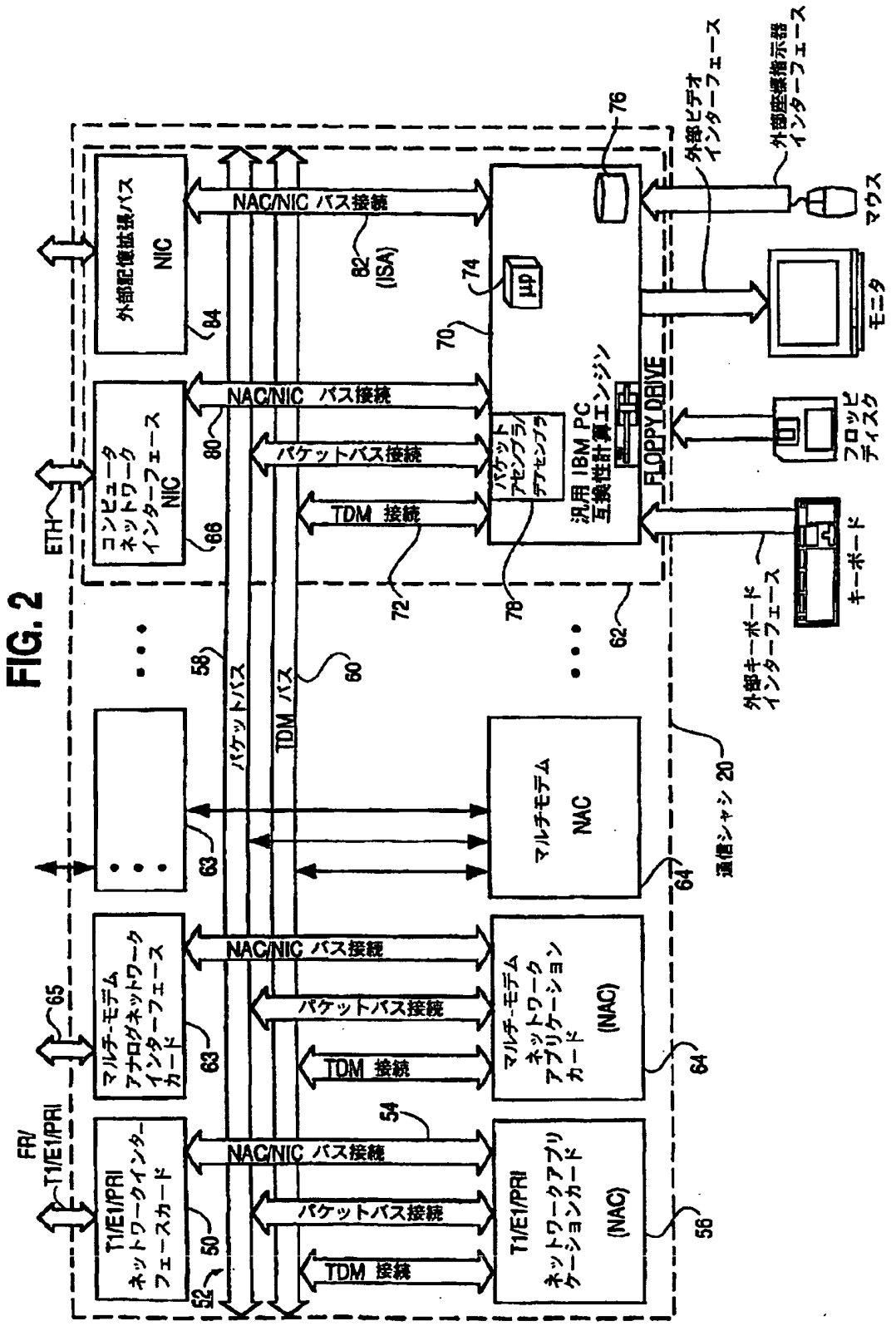
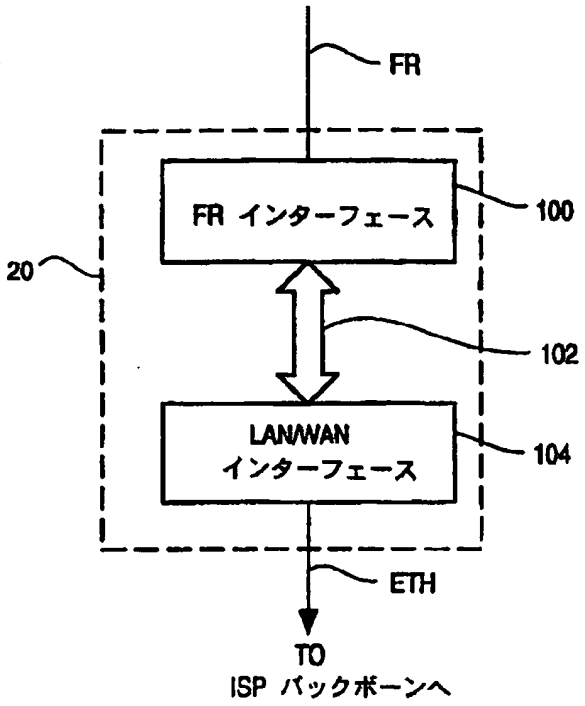

外部記憶拡張バス NIC
NAC/NIC バス接続
82 (ISA)
74
μp
70
76
外部ビデオ インターフェース
外部座標指示器 インターフェース
マウス
モニタ
84
コンピュータ ネットワーク インターフェース NIC
80
パケットバス接続
TDM 接続
66
ETH
パケット アセンブラ/ デアセンブラ
汎用 IBM PC 互換性計算エンジン
FLOPPY DRIVE
フロッピ ディスク
72
78
62
キーボード
外部キーボード インターフェース
58
パケットバス
TDM バス
60
通信シャシ 20
マルチモデム NAC
64
マルチ-モデム アナログネットワーク インターフェース カード
65
63
マルチ-モデム ネットワーク アプリケーション (NAC)
FR/ T1/E1/PRI
54
T1/E1/PRI ネットワークインター フェースカード
50
52
T1/E1/PRI ネットワークアプリ ケーションカード (NAC)
56

FIG. 2

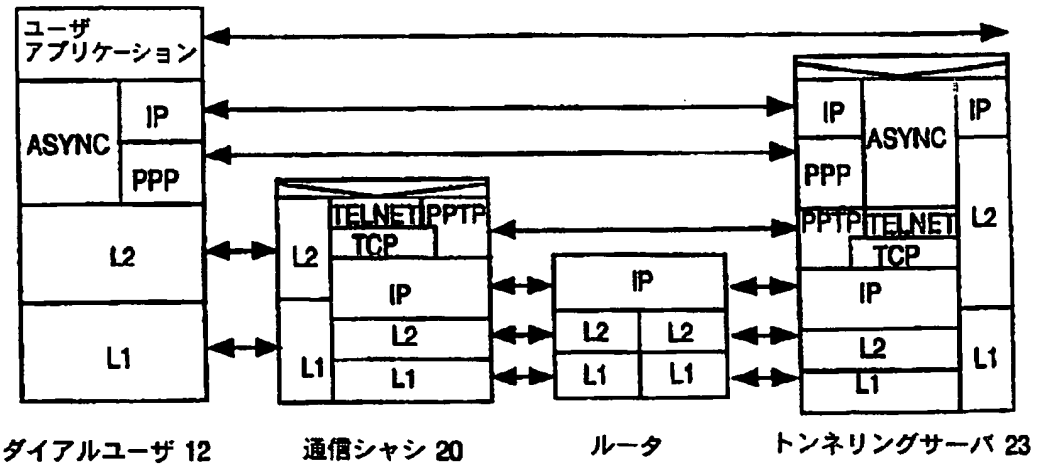
【図２】

FIG. 2A



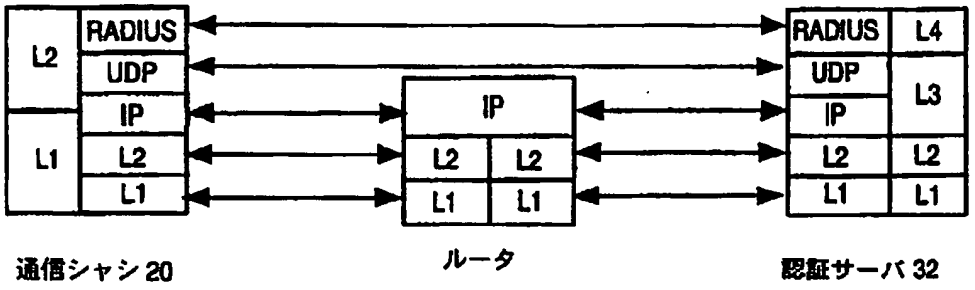
【図３】

FIG. 3



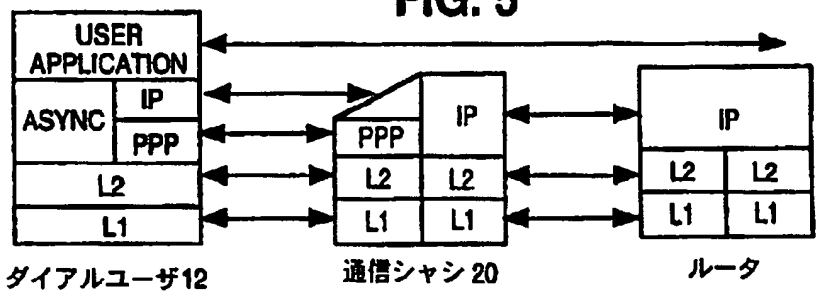
【図４】

FIG. 4



【図５】

FIG. 5



【図６】

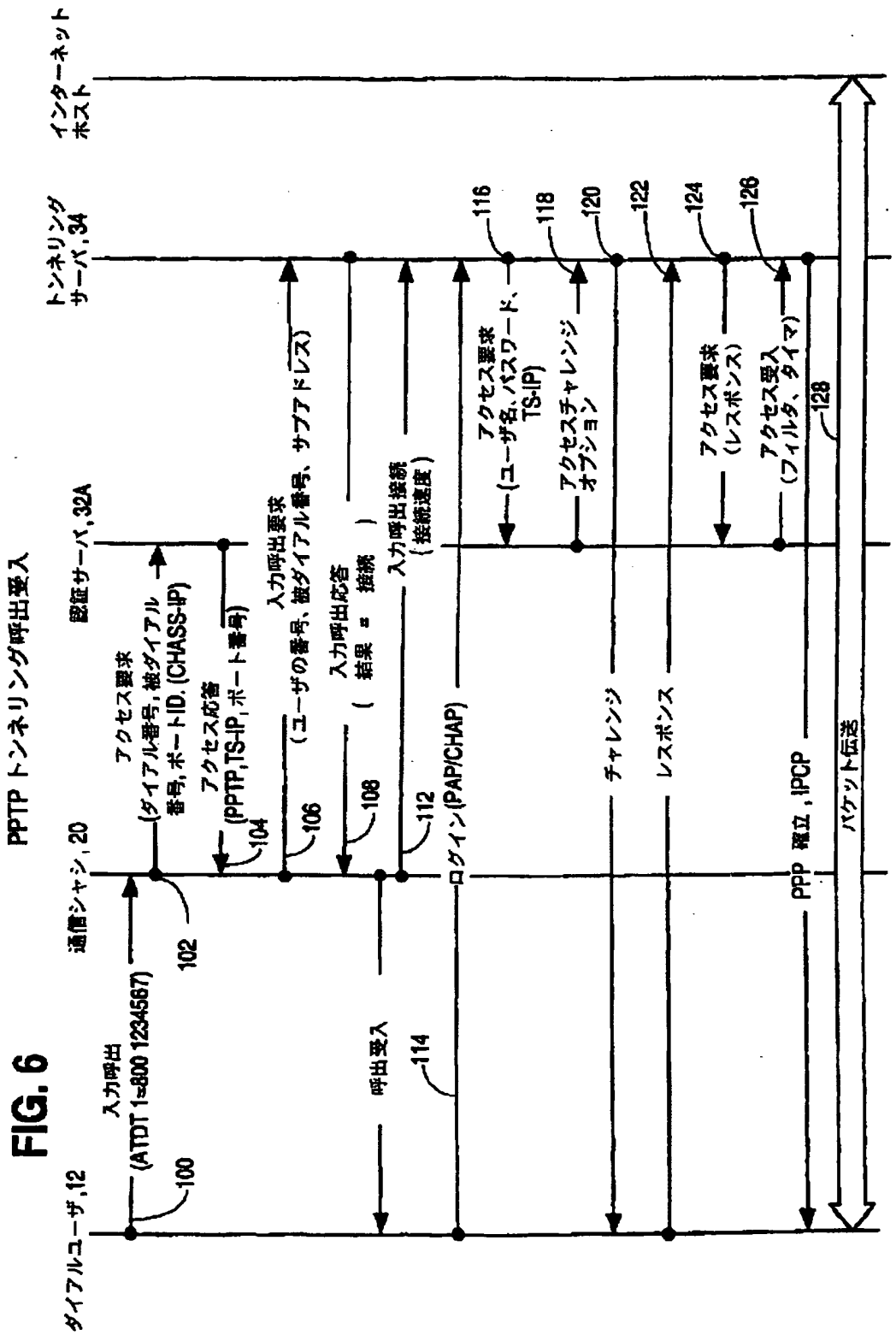
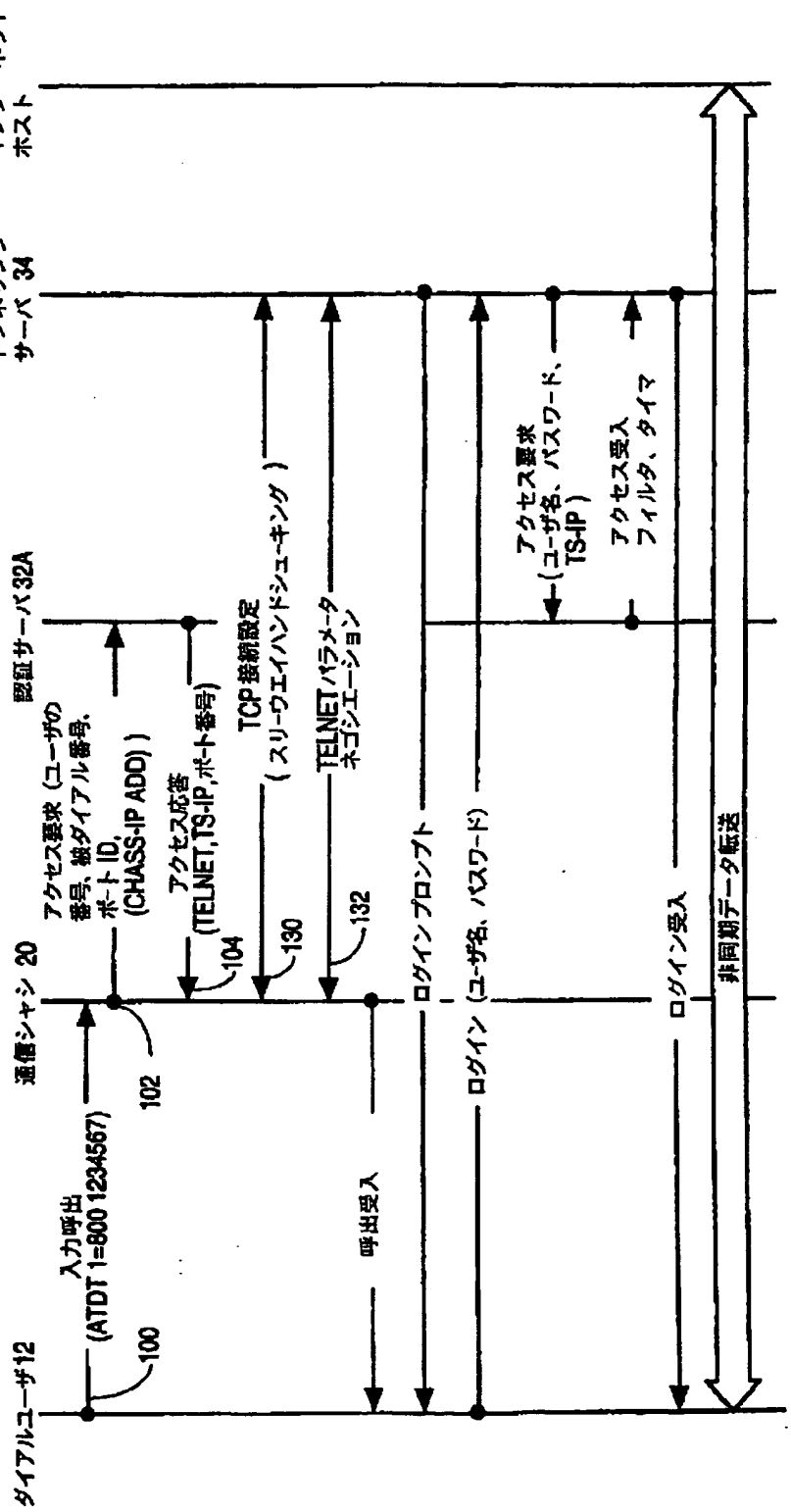

PPTP トンネリング呼出受入
ダイアルユーザ, 12
通信シャシ, 20
認証サーバ, 32A
トンネリングサーバ, 34
インターネットホスト
入力呼出
(ATDT 1=800 1234567)
100
102
アクセス要求
(ダイアル番号, 被ダイアル番号, ポートID, (CHASS-IP)
アクセス応答
(PPTP, TS-IP, ポート番号)
104
入力呼出要求
(ユーザの番号, 被ダイアル番号, サブアドレス)
106
入力呼出応答
(結果 = 接続)
108
呼出受入
114
入力呼出接続
(接続速度)
112
ログイン(PAP/CHAP)
アクセス要求
(ユーザ名, パスワード, TS-IP)
116
アクセスチャレンジ
オプション
118
120
チャレンジ
122
レスポンス
アクセス要求
(レスポンス)
124
アクセス受入
(フィルタ, タイマ)
126
128
PPP 確立, IPCP
パケット伝送

FIG. 6

【図７】

FIG. 7

TELNET　トンネリング呼出受入



【図８】

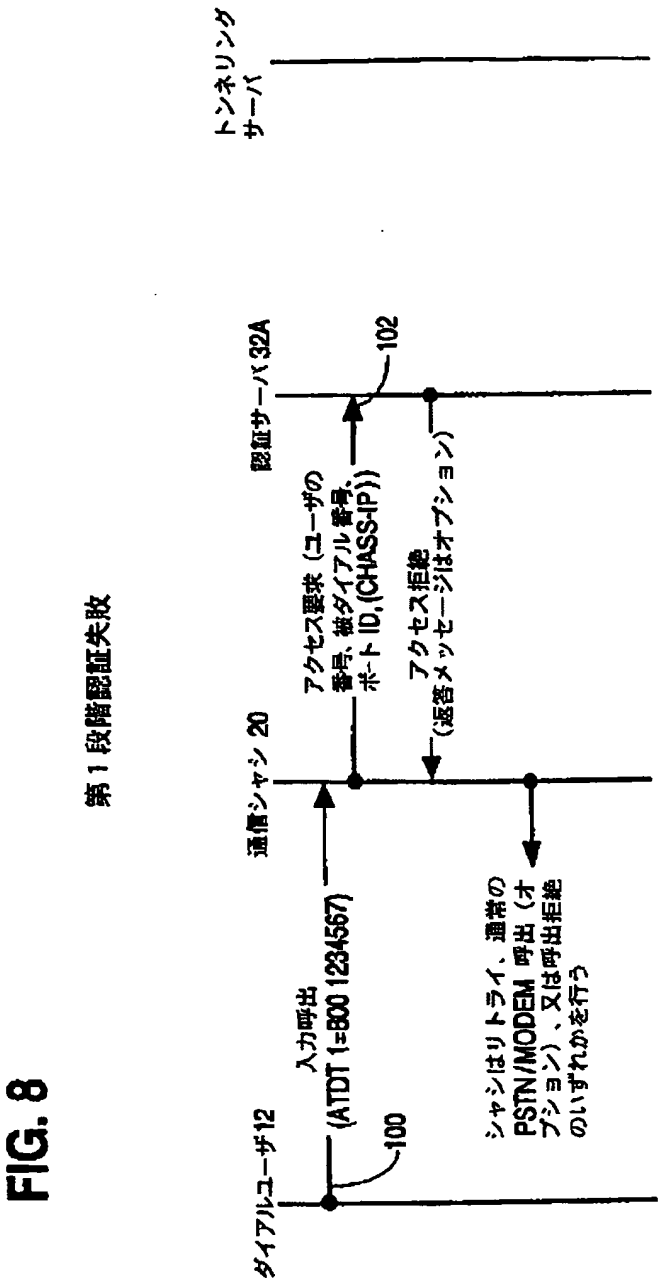


FIG. 8

第１段階認証失敗

【図９】

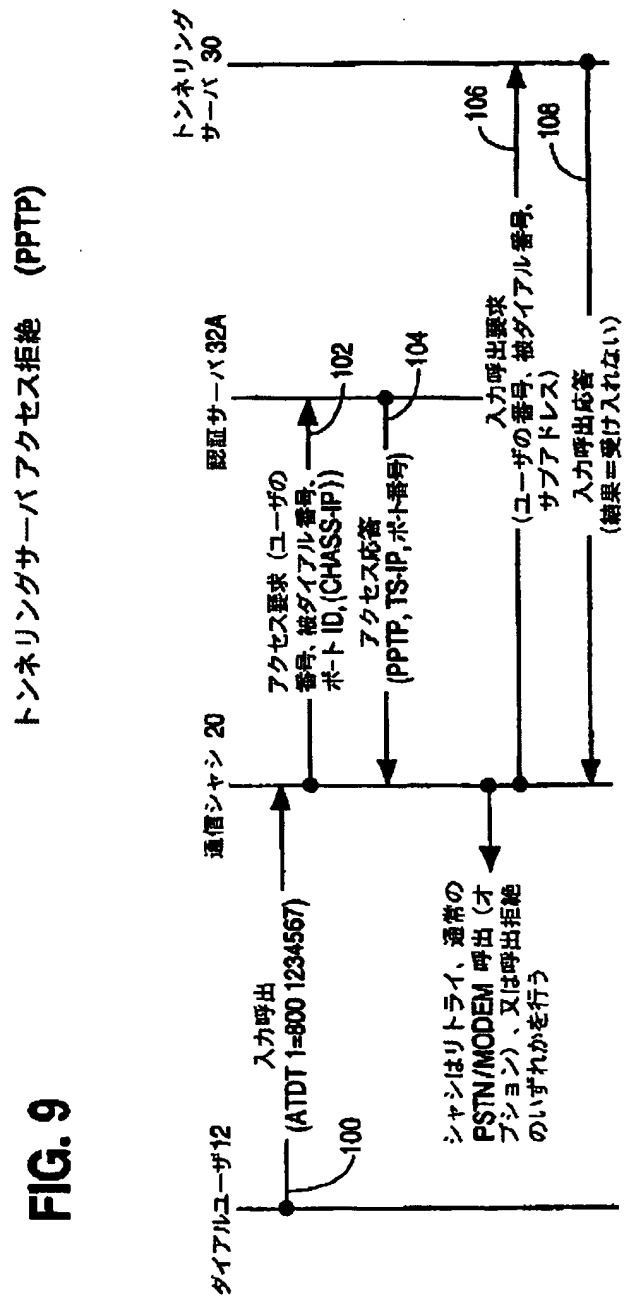


FIG. 9

トンネリングサーバアクセス拒絶　(PPTP)

【図１０】

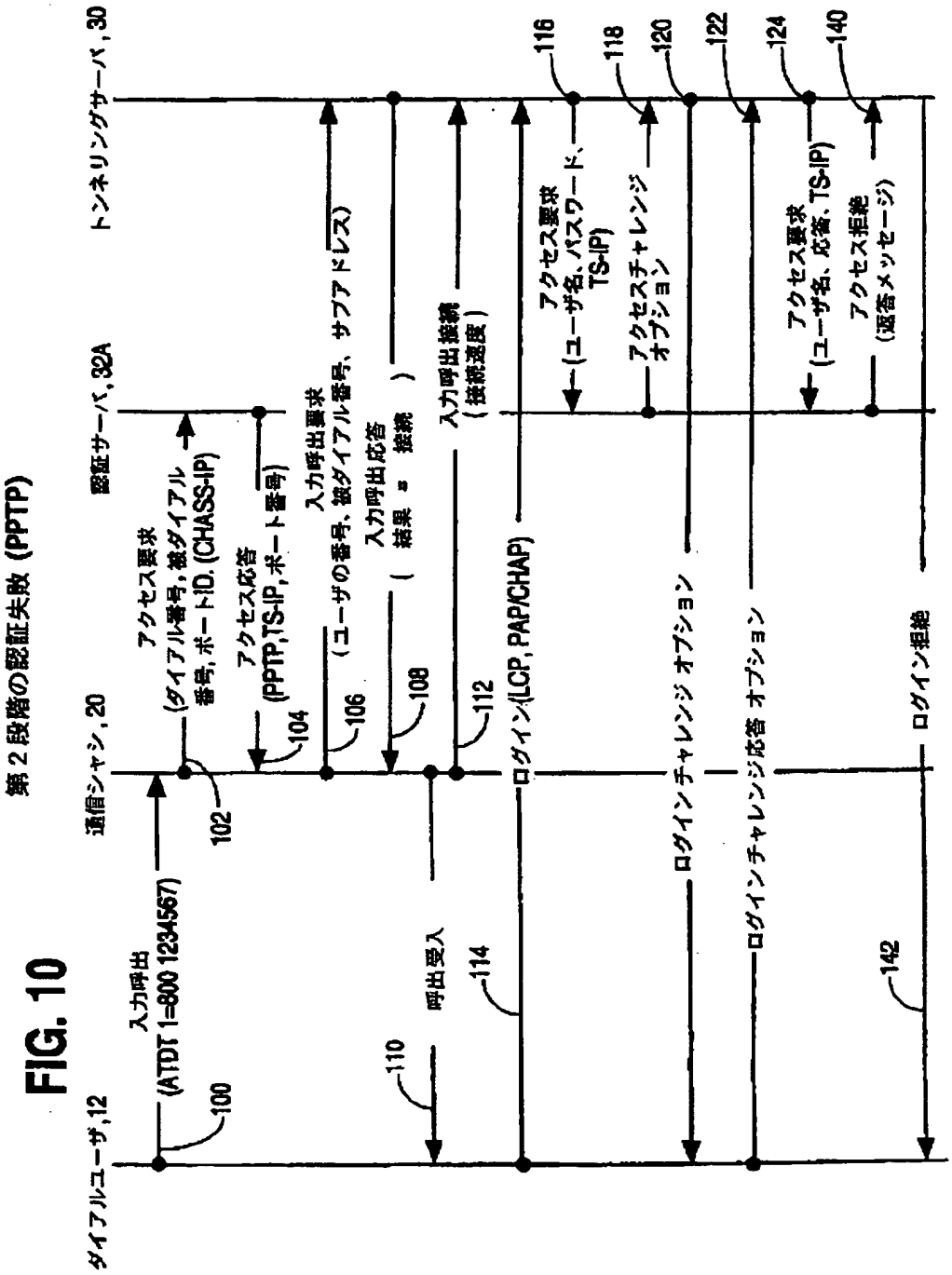

第２段階の認証失敗（PPTP）
ダイアルユーザ,12
通信シャシ,20
認証サーバ,32A
トンネリングサーバ,30
入力呼出
(ATDT 1=800 1234567)
100
アクセス要求
(ダイアル番号,被ダイアル番号,ポートID,(CHASS-IP)
102
アクセス応答
(PPTP,TS-IP,ポート番号)
104
入力呼出要求
(ユーザの番号,被ダイアル番号,サブアドレス)
106
入力呼出応答
(結果＝接続)
108
呼出受入
110
入力呼出接続
(接続速度)
112
ログイン(LCP,PAP/CHAP)
114
アクセス要求
(ユーザ名,パスワード,TS-IP)
116
アクセスチャレンジ
オプション
118
ログインチャレンジ オプション
120
ログインチャレンジ応答 オプション
122
アクセス要求
(ユーザ名,応答,TS-IP)
124
アクセス拒絶
(返答メッセージ)
140
ログイン拒絶
142

FIG. 10

【図１１】

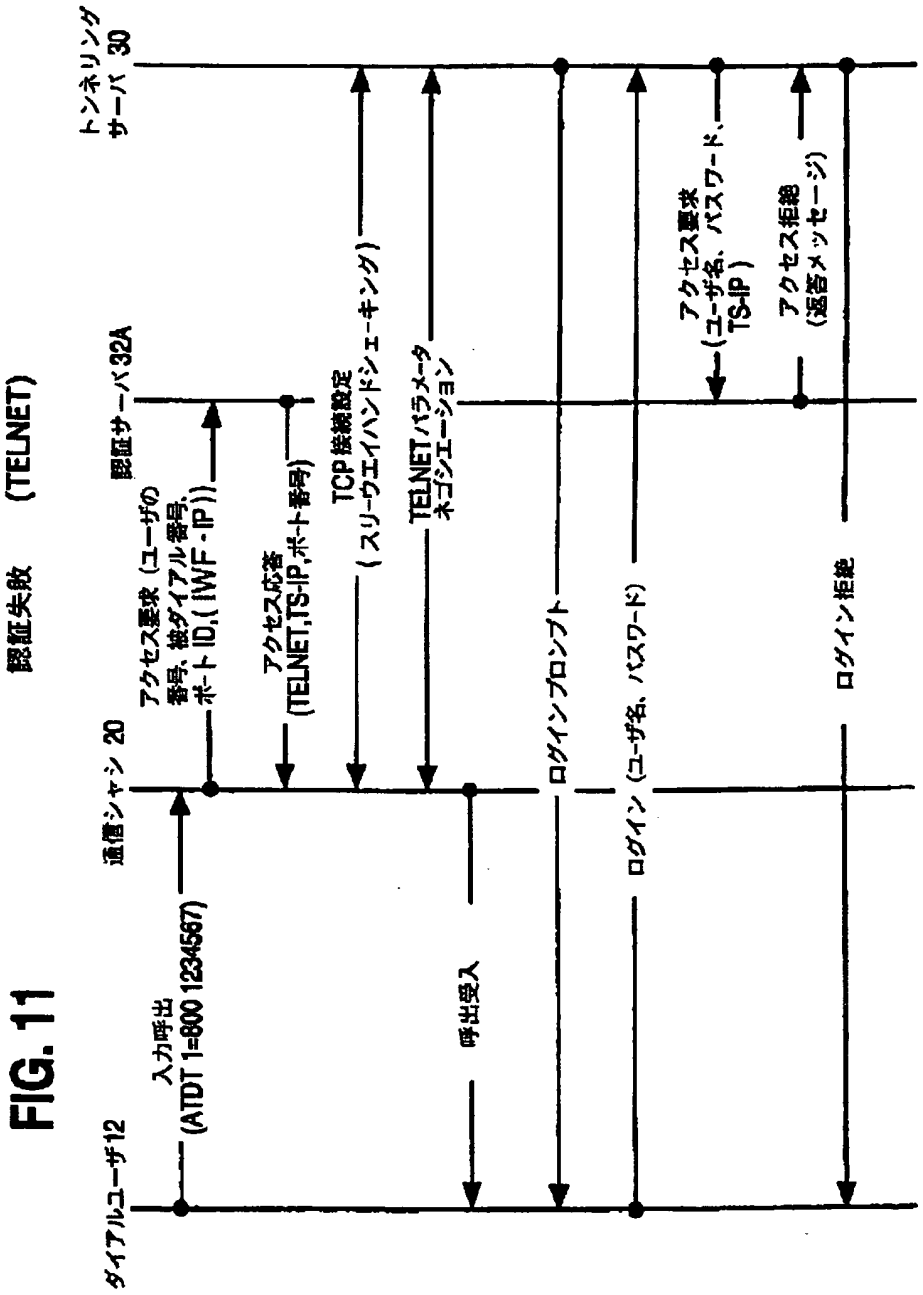


FIG. 11
認証失敗 (TELNET)
ダイアルユーザ12
通信シャシ 20
認証サーバ32A
トンネリング サーバ 30
入力呼出 (ATDT 1=800 1234567)
アクセス要求 (ユーザの番号、被ダイアル番号、ポートID、(IWF-IP))
アクセス応答 (TELNET,TS-IP,ポート番号)
TCP接続設定 (スリーウエイハンドシェーキング)
TELNETパラメータネゴシエーション
呼出受入
ログインプロンプト
ログイン (ユーザ名、パスワード)
アクセス要求 (ユーザ名、パスワード、TS-IP)
アクセス拒絶 (通告メッセージ)
ログイン拒絶

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/US 98/13858

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	VARMA V K ET AL: "ARCHITECTURE FOR INTERWORKING DATA OVER PCS" IEEE COMMUNICATIONS MAGAZINE, vol. 34, no. 9, September 1996, pages 124-130, XP000627245 see abstract see page 126, left-hand column, line 12 - page 127, left-hand column, line 8 see page 128, left-hand column, line 23 - page 128, right-hand column, line 9 see page 129, left-hand column, line 52 - page 130, left-hand column, line 14 see figures 2,7,10 --- -/--	1-8,17, 18

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
16 November 1998	23/11/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Lázaro López, M.L.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intl. ational Application No
PCT/US 98/13858

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 762 261 A (CADIX INC) 12 March 1997 see abstract see column 2, line 38 - column 4, line 20 see column 8, line 42-49 see column 9, line 6-9 see figures 1A,1B	9,11
A	WO 95 08900 A (NOKIA TELECOMMUNICATIONS OY ;WARSTA MARKUS (FI); JOKIAHO TIMO (FI)) 30 March 1995 see abstract see page 4, line 1-12 see page 4, line 24 - page 5, line 25 see page 5, line 34 - page 6, line 8 see page 6, line 14 - page 9, line 16 see page 9, line 25 - page 10, line 24 see figure 1	1-8
A	KYLAENPAEAE M ET AL: "NOMADIC ACCESS TO INFORMATION SERVICES BY A GSM PHONE" COMPUTERS AND GRAPHICS, vol. 20, no. 5, 1 September 1996, pages 651-658, XP002037372 see abstract see page 652, left-hand column, line 16-30 see page 653, left-hand column, line 5-30	1,17
A	PERKINS C ET AL: "IMHP: A mobile host protocol for the Internet" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 27, no. 3, December 1994, page 479-491 XP004037981 see abstract see page 483, right-hand column, line 1 - page 486, left-hand column, line 23	2,3, 8-13,16

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ational Application No
PCT/US 98/13858

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0762261 A	12-03-1997	JP 9081518 A	28-03-1997
		JP 9081519 A	28-03-1997
		JP 9081520 A	28-03-1997
		US 5706427 A	06-01-1998
WO 9508900 A	30-03-1995	FI 934115 A	21-03-1995
		AU 678534 B	29-05-1997
		AU 7658694 A	10-04-1995
		CN 1133666 A	16-10-1996
		EP 0720806 A	10-07-1996
		JP 9505951 T	10-06-1997

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04M 3/00		H04L 11/00	310C	
11/00	303	H04B 7/26	109M	
H04Q 7/38			109S	

(81)指定国　EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

【要約の続き】
トワークへのアクセスを許可する、という各ステップを有する。